高职高专计算机教学改革 新 体 系 规划教材

计算机网络安全技术案例教程

耿　杰　主编

清华大学出版社

高职高专计算机教学改革新体系规划教材

计算机网络安全技术案例教程

耿　杰　主　编
钱　亮　张宏宪　田　岭　白悍东　副主编

清华大学出版社
北　京

内 容 简 介

本书以 Windows Server 2003 为平台，通过实用的网络安全案例介绍计算机网络安全技术，使学生可以对网络安全知识学以致用。在内容的选取、组织与编排上，强调技术性、先进性、实用性，淡化理论，突出实践，强调应用。

本书共分为 9 章，内容如下：网络安全概述，通信协议与安全，数据加密技术，Windows Server 2003 的安全，防火墙技术，入侵检测技术，网络病毒的防范与清除，网络攻防技术，Web 安全技术。

本书既可以作为高职高专院校网络相关专业及电子商务等专业学习计算机网络安全技术的教材，也可以单独作为实验指导用书；同时，它还是一本实用的技术指导书，可以作为社会培训教材。

图书在版编目(CIP)数据

计算机网络安全技术案例教程/耿杰主编. --北京：清华大学出版社，2013
高职高专计算机教学改革新体系规划教材
ISBN 978-7-302-31213-0

Ⅰ. ①计…　Ⅱ. ①耿…　Ⅲ. ①计算机网络－安全技术－高等职业教育－教材　Ⅳ. ①TP383.08

中国版本图书馆 CIP 数据核字(2013)第 001762 号

责任编辑：陈砺川
封面设计：傅瑞学
责任校对：刘　静
责任印制：宋　林

出版发行：清华大学出版社
　网　　址：http://www.tup.com.cn，http://www.wqbook.com
　地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
　社 总 机：010-62770175　　**邮　　购**：010-62786544
　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
　课件下载：http://www.tup.com.cn，010-62795764
印 刷 者：三河市君旺印装厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.75　　**字　　数**：386 千字
版　　次：2013 年 10 月第 1 版　　**印　　次**：2013 年 10 月第1 次印刷
印　　数：1～3000
定　　价：33.00 元

产品编号：050613-01

前言

FOREWORD

编者在多年教学和实践经验的基础上，结合当前计算机网络安全技术的新成果，对计算机网络安全技术相关知识作了系统的介绍。本书以案例为依托，结合目前企业对网络安全技术的需求，主要介绍了以下内容：网络安全概述；通信协议与安全；数据加密技术；Windows Server 2003 的安全；防火墙技术；入侵检测技术；网络病毒的防范与清除；网络攻防技术；Web 安全技术。

本书具有如下特色。

以适应高职高专教学改革的需要为目标，充分体现高职高专特色，努力从内容到形式上有所创新和突破，其最大特点就是以企业需求为导向，讲究实用性。

在内容选取上，坚持集先进性、科学性和实用性为一体，尽可能选取最新、最实用的技术，满足以"提高学生能力为主"的高职高专教学的需要。

在考虑教材内容深浅程度时，把握理论够用、侧重实践、由浅入深的原则，以使学生分层分步骤掌握所学的知识。

在教材结构的安排上，采用实例引导和任务驱动模式作为教材编写的主干线，从知识—案例—练习—实训，逐渐展开内容，通过案例使知识具体化，增强对网络安全技术的感性认识，通过练习和实训来巩固和深化所学的知识，最后达到学习知识、培养能力的目的。本书案例丰富、典型，针对性强，能够很好地满足读者对知识和技能的需求。

本书既可以作为高职高专院校网络相关专业及电子商务等专业学习计算机网络安全技术的教材，也可以作为实验指导用书，同时也可以作为社会培训班用书。

在本书的编写过程中，编者参阅了大量的网上资料和出版的论文、教材、专著等，在此向这些作品的作者表示深深的敬意和感谢！

本书由耿杰担任主编并负责全书的统稿工作，钱亮、张宏宪、田岭、白悍东作为本书的副主编做了很多重要的工作，另外，彭庆红也参与了本书的编写。

由于作者水平有限，书中难免有不妥和错误之处，恳请广大读者指正。

目录

CONTENTS

第8章 网络攻防技术 /200

第9章 Web安全技术 /233

第 1 章 网络安全概述

Chapter 1

知识目标

- 理解网络安全的定义。
- 掌握网络面临的各种安全威胁。
- 了解产生网络安全威胁的原因。
- 了解计算机系统的安全级别。

技能目标

- 能识别网络威胁的类别。
- 能使用网络工具对计算机系统进行漏洞扫描。
- 掌握常用 DOS 命令的操作方法。

随着网络技术的不断发展，网络在人们生活中已经占有一席之地，为人们的生活带来了极大的方便。然而，网络也不是完美无缺的，它在给人们带来惊喜的同时，也带来了威胁。计算机犯罪、黑客、有害程序和后门等问题严重威胁着网络的安全。目前，网络安全问题已经在许多国家引起了普遍关注，成为当今网络技术的一个重要研究课题。

1.1 什么是网络安全

目前，Internet 几乎覆盖了世界各地，容纳了数十万个网络，为几十亿用户提供了形式多样的网络与信息服务。除了广泛应用的 Web 网页、E-mail、新闻论坛等文本信息的交流与传播之外，网络电话、网络传真、视频等通信技术都在迅猛地发展。在信息化社会中，计算机网络将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络的依赖日益增强。人们依靠计算机网络系统接收和处理信息，实现相互间的联系和对目标的管理、控制。通过网络交流信息、获得信息已成为现代信息社会的一个主要特征。网络正改变着人们的工作方式和生活方式。

科技进步在造福人类的同时，也带来了新的危害。随着网络的开放性、共享性和互联程度的扩大，特别是 Internet 的出现，网络变得越来越重要，对社会的影响也越来越大，随之而来的是利用计算机网络犯罪的情况越来越严重，已经严重地危害着社会的发展和国家的安全。

1989 年 10 月,有人为了抗议钚驱动的伽利略探测器的发射而制造 WANK(Worms Against Nuclear Killers)蠕虫入侵 NASA(美国宇航局),这是历史上有记载的第一次系统入侵,造成了约 50 万美元的损失。

1996 年 8 月 14 日,美国发生一起计算机病毒入侵计算机网络的事件,几千台计算机被病毒感染,Internet 不能被正常访问。政府不得不立即做出反应,国防部成立了计算机快速行动小组。这次病毒事件导致的直接经济损失超过 1 亿美元。

1994 年底,俄罗斯黑客弗拉米尔与其同伙从圣彼得堡的一家小软件公司的联网计算机上向美国 CITYBANK 银行发动了一连串的攻击,通过电子转账方式,从 CITYBANK 银行在纽约的计算机主机里窃取了 1100 万美元。

2000 年 1 月,一个昵称为 Maxim 的黑客侵入 CDUniverse. com 购物网站并窃取了 30 万份信用卡资料。

2003 年 3 月 21 日,黑客侵入了江苏某信息网的多台服务器,破译了密码数据库,获得了网络工作人员的口令和 300 多个合法用户的账号与密码,并将这些账号与密码公布于众。

2008 年 2 月,一黑客利用无线刷卡设备的漏洞入侵了美国两家大型连锁超市 Hannaford 和 Sweetbay,盗窃了 1800 份完整信用卡资料和 420 万个信用卡的部分资料。

事实上,以上这些网络入侵事件只是实际发生的网络入侵事件中非常微小的一部分,有相当多的网络入侵或攻击并没有被发现,或者出于各种各样的原因未被公开。据统计,商业信息被窃取的事件在每月以 260%的速度增加。社会上每公开报道一次网络入侵事件的背后,有无数例网络入侵事件是不被公众所知的。

面对越来越严重的计算机网络安全的威胁,必须采取措施来保证计算机网络的安全。但是现有的计算机网络大多数在设计的开始都忽略了安全问题。即使考虑了安全问题,大部分都是把安全机制建立在物理安全上。随着网络互联程度的扩大,这种安全机制对于网络环境来讲很脆弱。同时,目前网络上使用的协议,如 TCP/IP 协议,在制定之初也没有把安全考虑在内,所以网络协议本身就是不设防的,TCP/IP 协议中存在很多的安全问题,不能满足网络安全的要求。另外,网络的开放性和资源共享也是安全问题的一个主要根源,解决这个问题主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

一个安全的网络体系至少应包括三类措施,即法律措施、技术措施、政策措施。面对危害计算机网络安全的种种威胁,仅仅利用物理上和政策上的手段是十分有限和困难的,因此,也应采用逻辑上的措施,即研究开发有效的网络安全技术,例如,安全协议、密码技术、数字签名、防火墙、安全管理、安全审计等,以防止网络上传输的信息被非法窃取、篡改、伪造,保证其保密性和完整性;防止非法用户的侵入,限制网络上用户的访问权限,保证信息存放的私有性。除了私有性和完整性之外,一个安全的计算机网络还必须考虑通信双方身份的真实性和信息的可用性。

计算机网络安全的目的是要保证网络上数据存储和传输的安全性。国内外很多研究机构为了解决这个问题做了大量的工作,主要有数据加密、身份认证、数字签名、防火墙、安全审计、安全管理、安全内核、安全协议、IC 卡、拒绝服务、网络安全性分析、网络信息安全监测和信息安全标准化等方面的研究。

1.1.1 计算机网络安全

计算机网络安全是指保持网络中的硬件、软件系统正常运行,使它们不因自然和人为的因素而被破坏、更改和泄露。网络安全主要包括物理安全、软件安全、信息安全和运行安全四个方面。

1. 物理安全

物理安全包括硬件、存储媒体和外部环境的安全。硬件是指网络中的各种设备和通信线路,如主机、路由器、服务器、工作站、交换机、电缆等;存储媒体包括磁盘、光盘等;外部环境则主要指计算机设备的安装场地、供电系统。保障物理安全,就是要保护这些硬件设施能够正常工作而不被损害。

2. 软件安全

软件安全是指网络软件及各个主机、服务器、工作站等设备所运行的软件的安全。保障软件安全,就是保护网络中的各种软件能够正常运行而不被修改、破坏和使用。

3. 信息安全

信息安全是指网络中所存储和传输数据的安全,主要体现在信息隐蔽性和防修改的能力上。保障信息安全,就是保护网络中的信息不被非法修改、复制、解密、使用等,也是保障网络安全最根本的目的。

4. 运行安全

运行安全指网络中的各个信息系统能够正常运行并能正常地通过网络交流信息。保障运行安全,就是通过对网络系统中的各种设备运行状况进行监测,发现不安全因素时,及时报警并采取相应措施,消除不安全状态以保障网络系统的正常运行。

网络安全的目的是为了确保网络系统的保密性、完整性和可用性。保密性要求只有授权用户才能访问网络信息;完整性要求网络中的数据保持不被意外或恶意地改变;可用性指网络在不降低使用性能的情况下仍能根据授权用户的需要提供资源服务。

1.1.2 网络安全的特征

由于网络安全受到威胁的多样性、复杂性及网络信息、数据的重要性,在设计网络系统时,应该努力达到安全目标。一个安全的网络具有下面五个特征:可靠性、可用性、保密性、完整性和不可抵赖性。

1. 可靠性

可靠性是网络安全最基本的要求之一,是指系统在规定条件下和规定时间内完成规定功能的概率。如果网络不可靠,经常出问题,这个网络就是不安全的。目前,对于网络可靠性的研究主要偏重于硬件可靠性方面。研制高可靠性硬件设备,采取合理的冗余备

份措施是最基本的可靠性对策。但实际上有许多故障和事故，与软件可靠性、人员可靠性和环境可靠性有关。如人员可靠性在通信网络可靠性中起着重要作用。有关资料表明，系统失效中很大一部分是由人为因素造成的。

2. 可用性

可用性是可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的，有时还要求具有时效性。网络必须随时满足用户通信的要求。从某种意义上讲，可用性是可靠性的更高要求，特别是在重要场合下，特殊用户的可用性显得十分重要。为此，网络需要采用科学、合理的网络拓扑结构，必要的冗余、容错和备份措施及网络自愈技术、分配配置和负荷分担、各种完善的物理安全和应急措施等，从满足用户需求出发，保证通信网络的安全。在网络环境下，拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

3. 保密性

保密性指防止信息泄露给非授权个人或实体。信息只为授权用户使用，保密性是对信息的安全要求。它是在可靠性和可用性的基础上，保障网络中信息安全的重要手段。对于敏感用户信息的保密，是人们研究最多的领域。由于网络信息会成为黑客、计算机犯罪、病毒，甚至信息战的攻击目标，已受到了人们越来越多的关注。

4. 完整性

完整性也是面向信息的安全要求。它是指信息不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等操作破坏的特性。它与保密性不同，保密性是防止信息泄露给非授权的人，而完整性则要求信息的内容和顺序都不受破坏和修改。用户信息和网络信息都要求完整性，例如，对于涉及金融的用户信息，如果用户账目被修改、伪造或删除，将带来巨大的经济损失。网络信息一旦被破坏，严重的还会造成通信网络的瘫痪。

5. 不可抵赖性

不可抵赖性也称不可否认性，是面向通信双方（人、实体或进程）信息真实的安全要求。它包括收发双方均不可抵赖。随着通信业务的不断扩大，电子贸易、电子金融、电子商务和办公自动化等许多信息处理过程都需要通信双方对信息内容的真实性进行认同，为此，应采用数字签名、认证，数据完备、鉴别等有效措施，以实现信息的不可抵赖性。

网络的安全不仅仅是防范窃密活动，其可靠性、可用性、完整性和不可抵赖性应作为与保密性同等重要的安全目标来实现。我们应从观念上、政策上做出必要的调整，全面规划和实施网络信息的安全。

1.2 网络安全面临的威胁

1.21 网络内部威胁

1. 计算机系统的脆弱性

计算机系统的脆弱性主要来自计算机操作系统的不安全性，在网络环境下，还来源于网络通信协议的不安全性。计算机系统有其自身的安全级别，有的计算机操作系统属于D级，这一级别的操作系统基本没有安全防护措施，它就像一个门窗大开的屋子，如DOS、Windows 3.x、Windows 95等操作系统，它们只能用于一般的桌面计算机系统，而不能用于安全性要求高的服务器的操作系统。UNIX系统和Windows NT达到了C2级别，其安全性远远高于Windows 95操作系统，而且主要用于服务器上。但这种操作系统仍然存在安全漏洞，因为这两种系统都存在超级用户，UNIX中是root，而Windows NT中是Administrator，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者，这样系统将面临巨大的危险。现在，人们正在研究一种新型的操作系统，在这种操作系统中没有超级用户，也就不会存在超级用户带来的问题。现在很多操作系统都使用静态口令，但口令还是有很大破解可能性的，而且不好的口令维护制度会导致口令丢失。口令丢失也就意味着安全系统的全面崩溃。

世界上没有能长久运行的计算机系统，计算机系统可能会因硬件故障或软件原因而停止运行或发生运行错误，或被入侵者利用并造成损失。硬盘故障、电源故障和主板芯片故障等都是人们应经常考虑的硬件故障问题。软件原因可能存在于操作系统中，更多的是存在于应用软件中。

2. 网络内部的威胁

对网络内部的威胁主要来自网络内部的用户，这些用户试图访问那些不允许使用的资源和服务器。这种威胁可以分为如下两种情况。

(1) 有意的安全破坏，入侵者的攻击和计算机犯罪就是属于这一类。这是计算机网络所面临的最大威胁，此类威胁还可以分为主动攻击和被动攻击两种情况，主动攻击是指计算机网络的内部用户以各种方式有选择地破坏信息的有效性和完整性，而被动攻击则是在不影响网络正常工作的情况下，进行信息截获、窃取、破译等，目的是为了获得重要机密信息。

(2) 由于用户安全意识差造成的无意识的操作失误，使系统或网络发生故障或崩溃。如操作员安全配置不当造成的安全漏洞或隐患，用户安全意识不强，用户口令选择不慎或不恰当，用户将自己的账号保护不严或与别人共享等，都会对网络安全带来威胁和隐患，或者被非法入侵者加以利用，从而造成对系统的危害。

1.22 网络外部威胁

除了受到来自网络内部的安全威胁外，网络还受到来自外界的各种各样的威胁。网

络系统受到的威胁是多样的，因为在网络系统中可能存在许多种类的计算机和操作系统，采用统一的安全措施是不容易的，也是不可能的，而对网络进行集中安全管理则是一种好的方案。

安全威胁可以归结为物理威胁、网络威胁、身份鉴别、编程、系统漏洞等方面。

1. 物理威胁

物理安全是指保护计算机硬件和存储介质等设备和工作程序不遭受损失。常见的物理安全威胁有偷窃、垃圾搜寻和间谍活动等。物理安全是计算机系统和网络操作系统安全的最重要的方面。

办公室的计算机是偷窃者的主要目标之一。由于计算机或网络服务器中存储的数据信息的价值远远超过设备的价值，计算机偷窃行为对用户的损失可能成倍于被偷的设备的价值。因此，必须采取严格的防范措施以确保计算机设备不会被偷窃。入侵者可能会潜入计算机房，偷取计算机或计算机里的机密信息，也可能化装成计算机维修人员，趁管理员不注意时进行偷窃。当然，也可能是内部职员窃取他们不应该看到的信息，并把信息散布出去或卖给竞争对手。

千万不要小看了搜寻垃圾。在商业竞争中，有些人专门会搜寻竞争对手扔下的垃圾，以寻找一些机密信息。办公室的工作人员可能会把一些没经过任何安全处理的打印错误的文件扔进废纸篓，而这些文件就有可能落到竞争对手的手中，这样，机密信息便泄露了。

间谍活动是人们不能忽略的一种因素，现在商业间谍很多，而且一些商业机构可能会为击败对手而采取任何不道德的手段，有时政府机关也有可能卷入这种间谍活动当中。

2. 网络威胁

计算机网络的发展和使用对数据信息造成了新的安全威胁。在计算机网络中存在电子窃听，分布式计算机系统的特征使各种分离的计算机通过一些媒介相互连接在一起，进行相互通信，而且局域网一般是广播式的，只要把网卡模式设置成混合模式，网络上人人都可以收到发向任何人的信息。当然，也可以通过加密来解决这个问题，但目前强大的加密技术还没有在网络上广泛使用，况且加密也是有可能被破解的。

网络设备也可以造成网络的安全威胁。我国的很多个人网络用户都是通过调制解调器用电话线等方式拨号接入 Internet 或单位的局域网的，因为调制解调器也存在安全问题，入侵者可能通过电话线入侵到用户的网络中。

在 Internet 上还存在很多电子欺骗的现象，而这种电子欺骗的形式也是多种多样的，如一个公司可能会谎称一个站点是其公司的网站。在网络通信中，有的人可能冒充别人或冒充从另外一台机器访问某站点等，这样会很难辨别用户的真实身份。

3. 身份鉴别

目前，身份鉴别普遍存在于计算机系统当中，实现的方式各种各样，有的功能十分强大，有的则比较脆弱。其中，口令就是一种比较脆弱的身份鉴别手段，它的功能不是很强，但因为它实现起来比较简单，所以还是被广泛采用。计算机系统中的身份鉴别存在口令

圈套、口令破解和算法缺陷等安全威胁。

口令圈套是一种十分高明的诡计,它是一种靠欺骗来获取口令的手段。如登录欺骗,具体是写出一个运行起来像登录屏幕一样的代码模块,把它插入登录过程之前,这样,用户就会把用户名和登录口令告知程序,这个程序会把用户名和口令保存起来。除此之外,该代码还会告诉用户登录失败,并启动真正的登录程序,这样用户就不容易发现这个欺骗。

还有一种得到口令的方式是用密码字典或其他工具软件来暴力破解口令,有的用户选用的口令十分脆弱,如一个人的生日、电话号码、名字或单词等,这样攻击者就很容易强行破解。因此,系统管理员应对用户的口令进行严格审查,通常可以利用一些工具软件来检查口令是否达到系统管理的要求和规定。

口令输入后要正常工作必须满足一定的条件,当条件发生变化时,其口令算法程序就可能工作不正常。即当人们移植一种算法时,这种算法可能在人们工作环境下存在漏洞,这就是口令算法缺陷带来的安全隐患。

4. 编程

编程威胁主要有计算机病毒和特洛伊木马等。编程就是通过编制程序代码实施对系统的破坏。计算机病毒就是一种能进行自我复制的程序代码,它可以像生物病毒一样传染别的完好的程序。计算机病毒具有一定的破坏性,破坏性大小不一样,小的只是显示一些信息,影响用户使用计算机,而大的可能会让整个系统瘫痪。现在,Internet 上有很多种类的病毒,这些病毒在网络上不断地传播,严重危害 Internet 的安全。它可能通过不同的方式进入用户的计算机系统或网络系统,如下载软件、Java Applet 程序、ActiveX 和电子邮件等。

现在,在桌面系统中流行一种宏病毒,可以破坏 Word 文档,这种病毒存在于宏操作的软件中,如 Microsoft 的 Word 和 Excel 等软件。

逻辑炸弹是一种恶意代码,它可以让用户的系统瞬间崩溃,还会格式化硬盘或删除系统文件等。特洛伊木马也是一种恶意代码,但它和逻辑炸弹不同,它会把自己伪装成一个很正常的程序,在用户不知道的情况下破坏系统,具有很大的破坏性。

5. 系统漏洞

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误,这个缺陷或错误可以被不法者或者黑客利用,通过植入木马、病毒等方式来攻击或控制整个计算机,从而窃取其中的重要资料和信息,甚至破坏计算机系统。

漏洞影响到的范围很广,包括系统本身及其支撑软件、网络客户和服务器软件、网络路由器和安全防火墙等。换言之,在这些不同的软、硬件设备中都可能存在不同的安全漏洞问题。在不同种类的软、硬件设备,同种设备的不同版本之间,由不同设备构成的不同系统之间,以及同种系统在不同的设置条件下,都会存在不同的安全漏洞问题。

1.23 网络安全防范措施

系统的价值是由系统性能、安全管理花费的时间、使用性和复杂性决定的。许多系统设有系统“安全员”，专门管理和监控计算机系统设备的安全运转。安全措施有很多形式，如将操作系统设置成阻止用户读取未经批准的数据，不允许用户越权读取数据信息。它可以是计算机用户的工作步骤，如在碎纸机或者焚烧炉中处理所有的打印资料或磁介质，也可以以报警和日志的形式出现，如告诉管理员在什么时候有人试图闯入或闯入成功。安全措施还包括在操作人员接触秘密数据前，对他们进行广泛的安全检查。安全措施也可以是保障物理安全的形式，如门上锁和设报警系统以防止有人偷窃设备和存储介质等。

在安全环境中，许多安全措施相互加强，如果一层失败，则另一层将防止或最大限度地减少损害。下面是一些具体的措施。

1. 数据信息的备份

应经常备份或拷贝重要的数据，并将拷贝或备份保留在一个安全的地方，一旦失去原件就能使用备份。应该有规律地备份以便用户避免由于硬件的故障导致数据信息的丢失。提高可靠性是提高安全性的一种方法，备份就是一种提高系统可靠性的方法，它可以保证今天存储的数据明天还可以使用。由于计算机系统芯片或者电源的失效，甚至是火灾等可能引起系统的失误或破坏，备份将提高安全保障。

备份对于防范人为的破坏也至关重要。如果计算机系统被破坏，只要有数据备份，就可以在另一台计算机上恢复。备份系统是最常用的提高数据完整性的措施，备份工作可以手工完成，也可以自动完成，现有的操作系统都自带备份系统，但这种备份系统比较初级，如果对备份要求高，需要配置专门的备份系统。

2. 病毒检查

定期检查病毒并对移动存储介质或下载的文件或软件加以安全控制，最起码应在使用前对移动存储介质和下载的软件进行病毒检查，及时更新杀毒软件的版本，注意病毒流行的动向，及时发现正在流行的计算机病毒，并采取相应的措施进行防范。

3. 及时安装补丁程序

计算机操作系统和应用系统软件都会存在一些漏洞，这些漏洞可以通过软件商提供的补丁程序进行修正，因此，要及时安装各种安全补丁程序，不给入侵者任何可乘之机。系统的安全漏洞传播很快，若不及时修正，后果就难以预料。现在，一些大公司的网站上都有这种系统安全漏洞的说明，并有相应的解决方法，用户可以访问这些站点以获取有用的信息，或对软件进行自动更新。

4. 提高物理安全

保证计算机机房的安全是提高物理安全的重要保证，因为即使采取了网络安全或其

他安全措施,如果有人闯入机房,那么所有措施也都不是很管用了。

5. 设置 Internet 防火墙

Internet 防火墙是一种有效保证网络安全的技术,但一个维护很差的防火墙也不会有很大的作用,所以还需要有经验的人员进行管理和维护。虽然防火墙是网络安全体系中极为重要的一环,但它并不是万能的,虽然防火墙可以解决一些安全问题,但仍有很多危险是防火墙解决不了的。

防火墙不能防止内部的攻击,因为它只提供了网络边界的防卫,而内部人员可以滥用访问权限,从而引起安全事故。事实上,许多黑客入侵事件和 Internet 的关系很小,如一种常用的入侵手段是社会工程攻击,它就是靠欺骗获得一些可以破坏安全的信息来实施攻击的,如网络口令等。另外,一些用来传递数据的电话线也可能被作为入侵内部网络的途径。

有恶意的代码也是防火墙不能解决的问题之一,如 E-mail 和 Java 的使用为病毒和特洛伊木马的传播带来了方便。虽然现在的防火墙可以检查病毒和特洛伊木马,但这些防火墙只能阻挡已知的病毒程序,这就可能让新的特洛伊木马侵入系统。而且,特洛伊木马不仅来自网络,也可能来自光盘和移动存储设备,因此,要有相应的制度,对网络和磁盘进行严格的检查。

如果没有明确的信息安全制度,即使拥有再好的防火墙也没有用。在建立局域网时如果没有做好计算机的安全措施,当把局域网连入 Internet 时,就不能保证局域网的安全。

6. 审查日志

阅读审查日志文件,可以发现系统被入侵的痕迹,以便及时采取弥补措施,或追踪入侵者。对可疑活动一定要进行仔细分析,如有人在试图访问一些不安全的服务端口,有人利用 Finger、TFTP 或 Debug 等手段访问用户的邮件服务器,有人企图登录到用户的计算机,特别是试图登录到 Internet 的通用账户上。

7. 数据加密

现代加密技术很发达,为防止网络被窃听和劫持,可以对网络通信进行加密,对绝密文件更应该实施加密,以保证数据或数据通信的可靠和安全。



【案例】 与 Ping 命令相关的攻击与防范

案例分析

测试网络的命令 Ping(Packet Internet Grope,Internet 包探索器)是用于测试网络连接情况的程序。它发送一个 ICMP 响应请求消息给目的地,并报告是否收到所希望的 ICMP 应答,以便校验与远程/本地计算机的连接。

本案例中的攻击只需网中多台计算机同时在 Ping 命令后加上参数-t 对目标机进行

长时间测试,就攻击的意义而言就完成了一次 Ping 攻击,大量的数据包将会使目标机运行速度越来越慢,甚至瘫痪。在 DOS 环境中完成这个命令,命令格式如下。

```
Ping  目标 IP地址  -t
```

例如:

```
Ping 192.168.0.6 -t
```

下面进入防范 Ping 攻击的操作,该步骤通过添加 IP 策略完成。

操作步骤

第 1 步 添加 IP 安全策略。先在控制台中添加 IP 安全策略单元,添加步骤如下。

(1) 选择"开始"→"运行"命令,在出现的"运行"窗口中输入 mmc 并按 Enter 键,此时将打开"控制台 1"窗口,如图 1.1 所示。

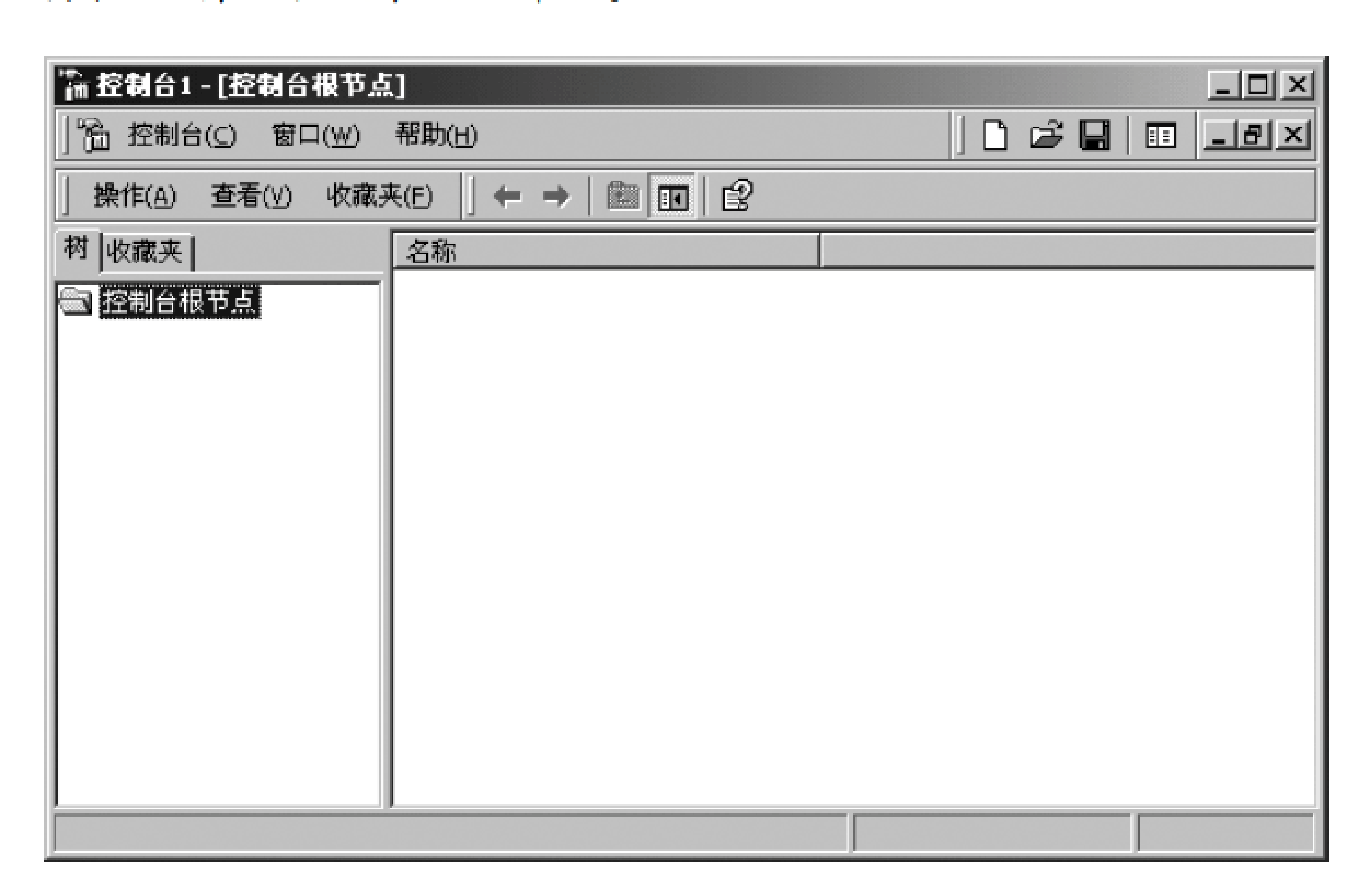


图 1.1 "控制台 1"窗口

(2) 在图 1.1 所示窗口依次单击"文件"→"添加/删除管理单元"命令,此时将打开"添加/删除管理单元"对话框,单击"添加"按钮,在弹出的"添加独立管理单元"对话框中的"管理单元"列表中双击"IP 安全策略管理",如图 1.2 所示。



图 1.2 "添加独立管理单元"对话框

(3) 这时将弹出"选择计算机或域"对话框,在此选中"本地计算机",然后单击"完成"按钮,最后依次单击"关闭"、"确定"按钮,返回"控制台 1"窗口,此时在"控制台根节点"下增加了"IP 安全策略,在本地机器"选项,如图 1.3 所示,这说明控制台中已经添加了

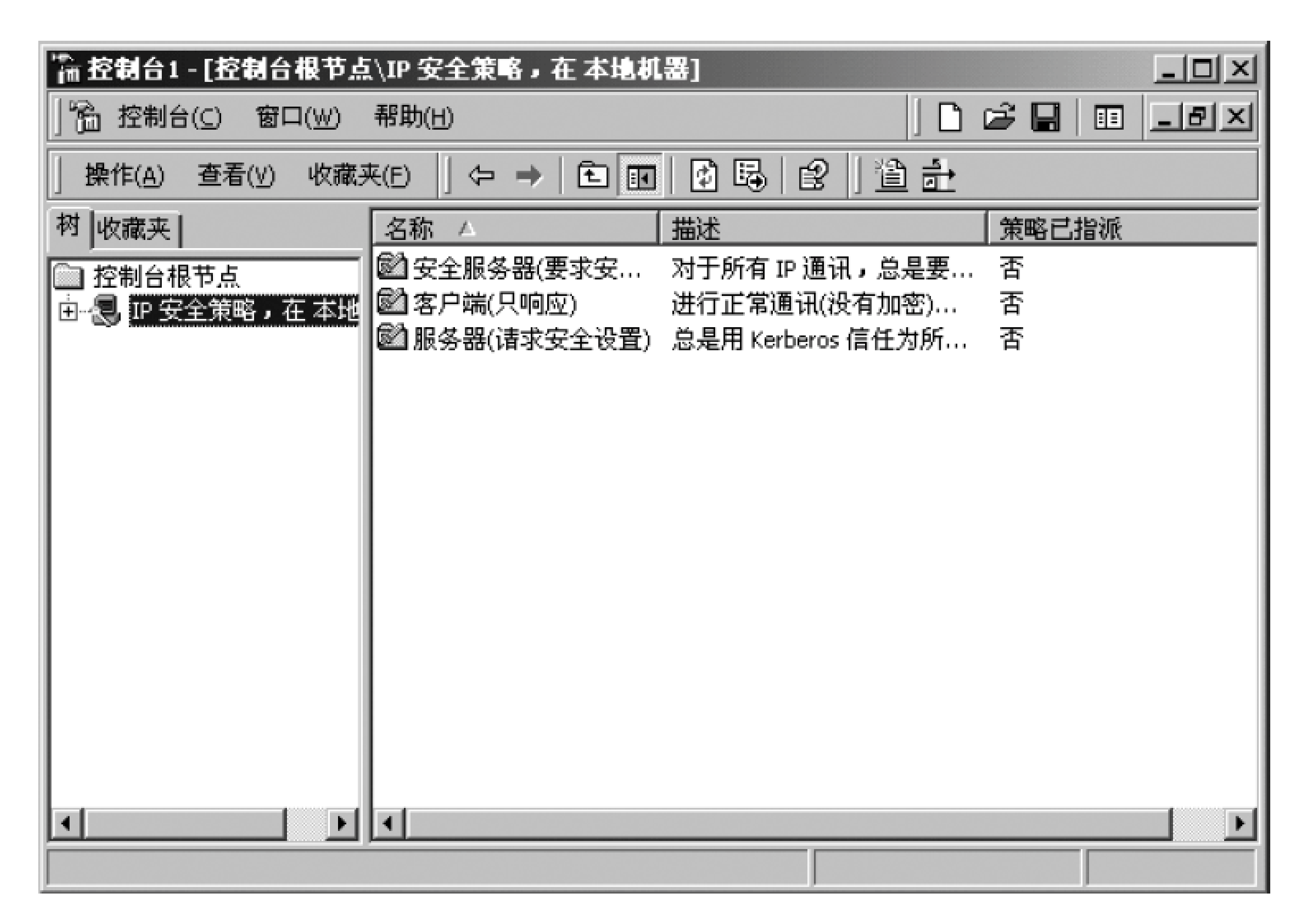


图 1.3　控制台根节点

IP 安全策略选项。

第 2 步　创建 IP 安全策略。在添加 IP 安全策略后，还要创建一个新的 IP 安全策略，步骤如下。

(1) 在图 1.3 中右击“IP 安全策略，在本地机器”选项，在快捷菜单中选择“创建 IP 安全策略”命令，打开“IP 安全策略向导”窗口。

(2) 单击“下一步”按钮，将出现要求指定 IP 安全策略名称及策略描述向导页面，在“描述”文本框中输入一个策略描述，如“禁止 ping”，如图 1.4 所示。

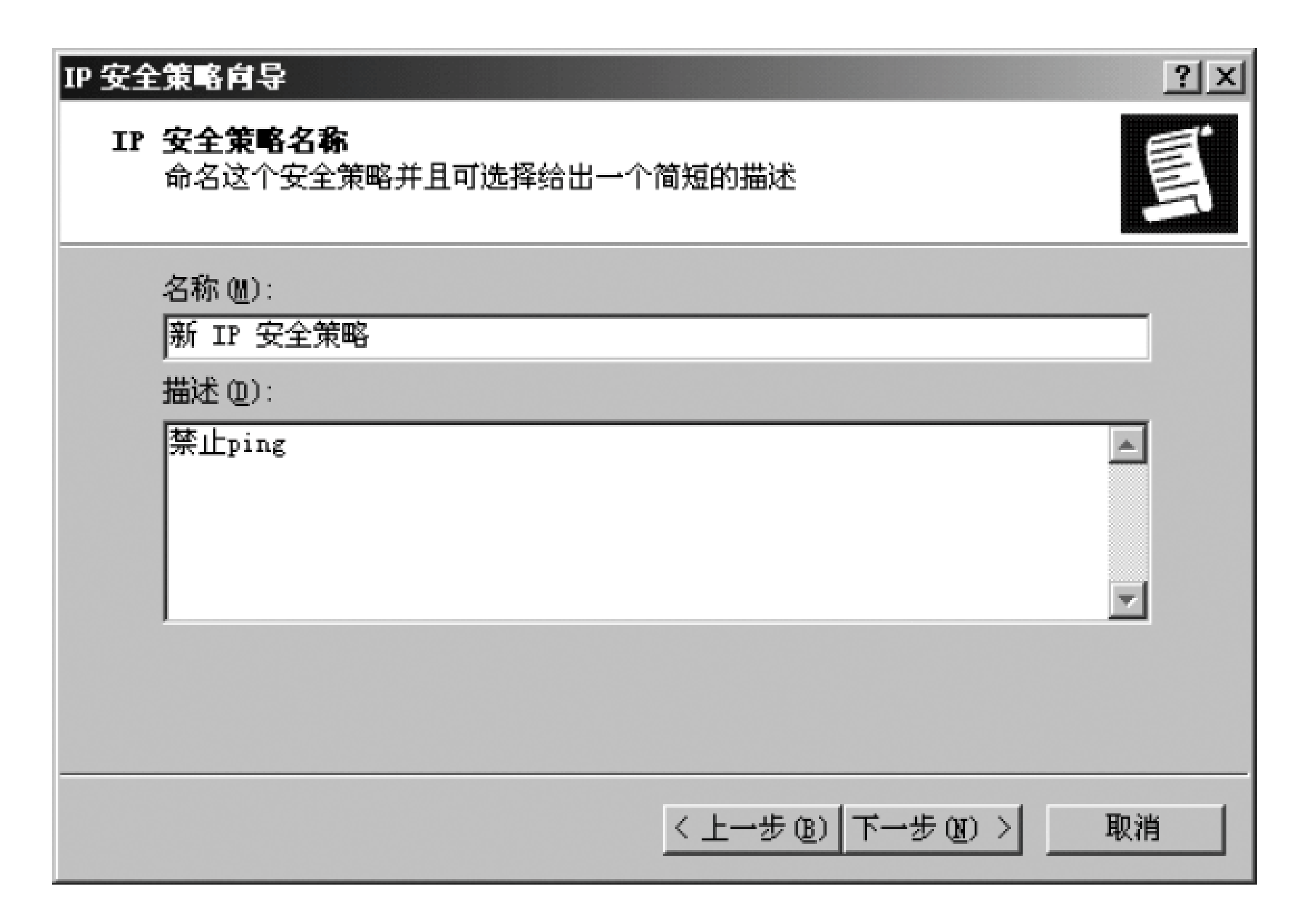


图 1.4　“IP 安全策略向导”窗口

(3) 单击“下一步”按钮，在出现的页面中选中“激活默认相应规则”选项，然后单击“下一步”按钮。

(4) 在出现的“默认响应规则身份验证方法”页面中选中“此字串用来保护密钥交换

(预共享密钥)"单选按钮,然后在下面的文本框中任意输入一段字符串(如"禁止 ping"),如图 1.5 所示。

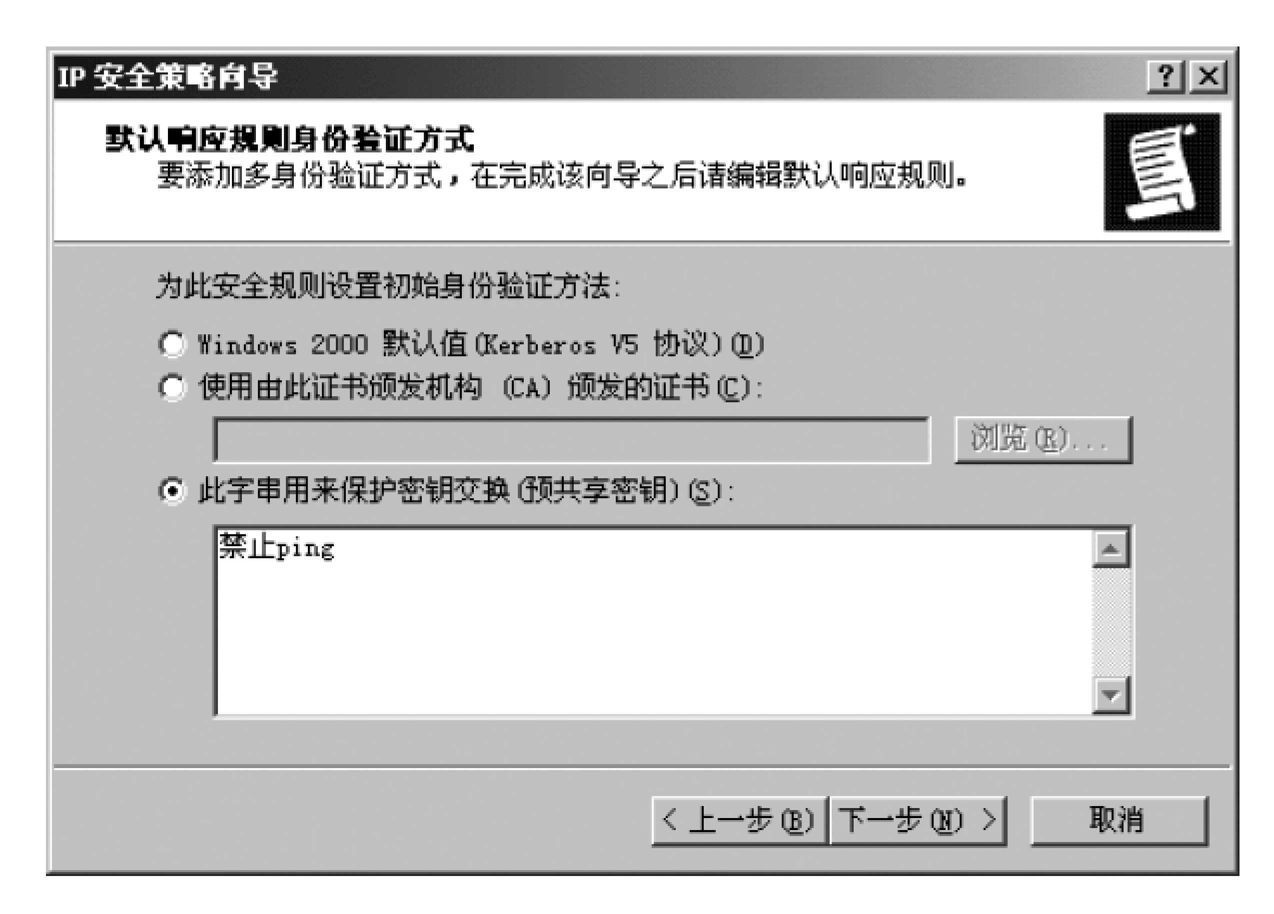


图 1.5 "默认响应规则身份验证方法"页面

(5) 单击"下一步"按钮,将出现完成"IP 安全策略向导"对话框,最后单击"完成"按钮即完成了 IP 安全策略的创建工作。

第 3 步 编辑 IP 安全策略属性。在以上 IP 安全策略创建后,在控制台中就会看到刚刚创建好的"新 IP 安全策略"选项。下面还要对其属性进行编辑修改,步骤如下。

(1) 在控制台中双击创建好的"新 IP 安全策略",将弹出"新 IP 安全策略 属性"对话框,如图 1.6 所示。



图 1.6 "新 IP 安全策略 属性"对话框

(2) 单击"添加"按钮,将弹出"安全规则向导"对话框,单击"下一步"按钮则进入"隧道终结点"页面,在此选择"此规则不指定隧道"选项。

(3) 单击"下一步"按钮,将出现"网络类型"页面,选中"所有网络连接"单选按钮,就能保证所有计算机都 Ping 不通该主机了,如图 1.7 所示。

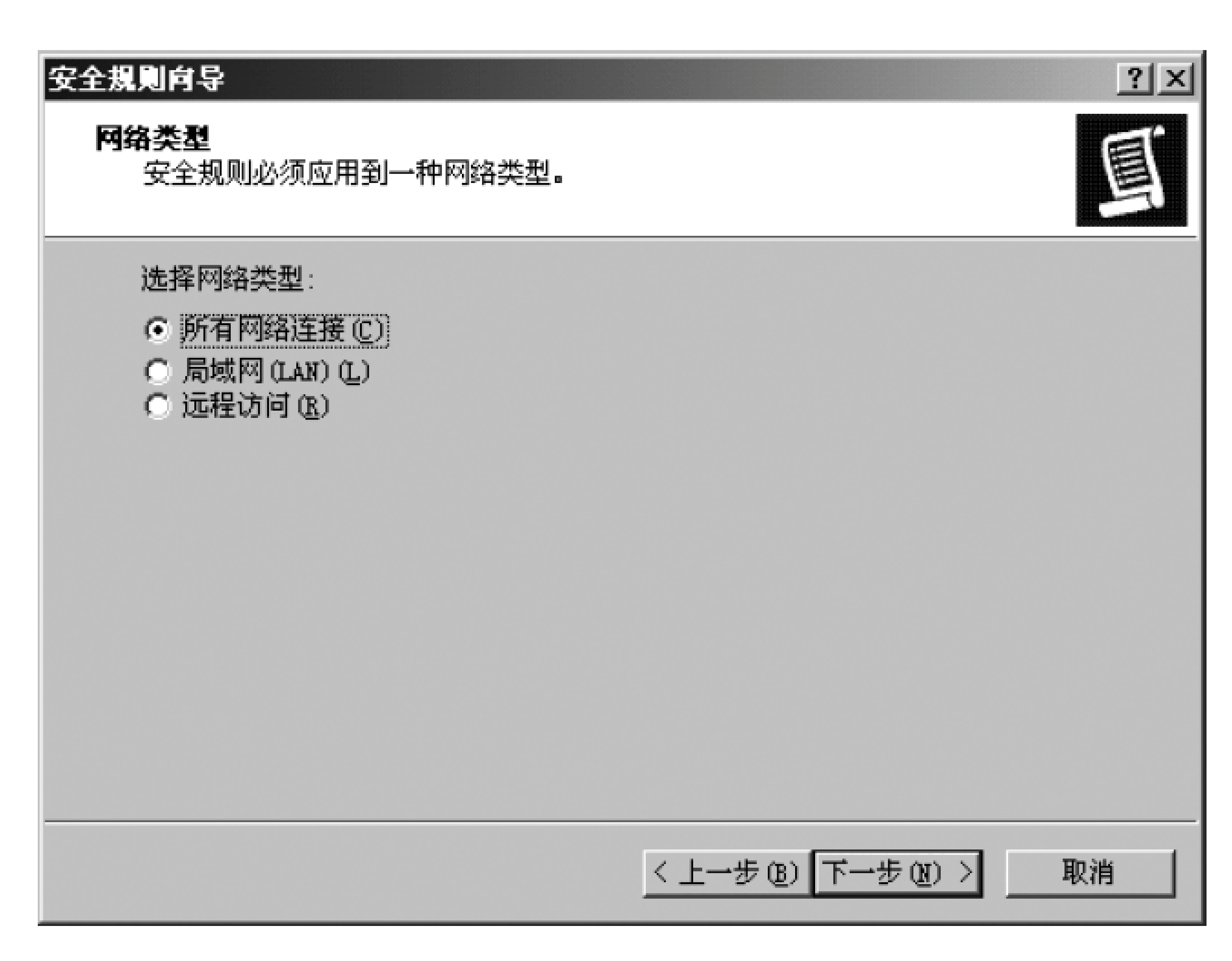


图 1.7 选中"所有网络连接"单选按钮

(4) 单击"下一步"按钮,将出现"身份验证方法"页面,选中"此字串用来保护密钥交换(预共享密钥)"单选按钮,然后在下面的文本框中输入"禁止 ping",如图 1.8 所示。

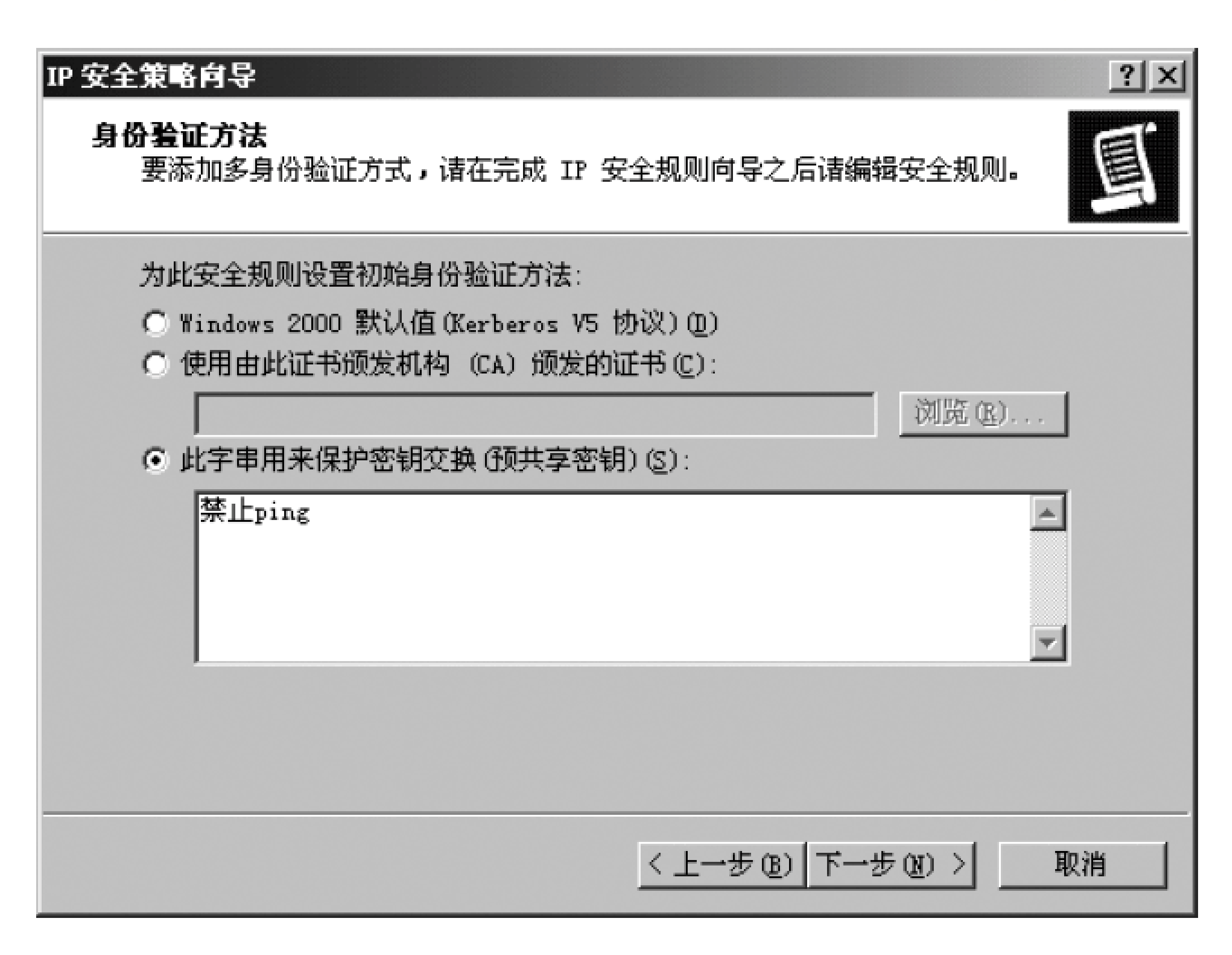


图 1.8 "身份验证方法"页面

(5) 单击"下一步"按钮,在打开的"IP 筛选器列表"对话框中单击"添加"按钮,打开"IP 筛选器列表"对话框,如图 1.9 所示。

(6) 单击"添加"按钮,打开"筛选器向导"窗口,单击"下一步"按钮,打开"IP 通信源"页面,在该页面中设置"源地址"为"我的 IP 地址",如图 1.10 所示。

(7) 单击"下一步"按钮,在弹出的"IP 通信目标"页面中设置"目标地址"为"任何 IP 地址",则任何 IP 地址的计算机都不能 Ping 用户的机器,如图 1.11 所示。

(8) 单击"下一步"按钮,在出现的"IP 协议类型"页面中设置"选择协议类型"为 ICMP,如图 1.12 所示。

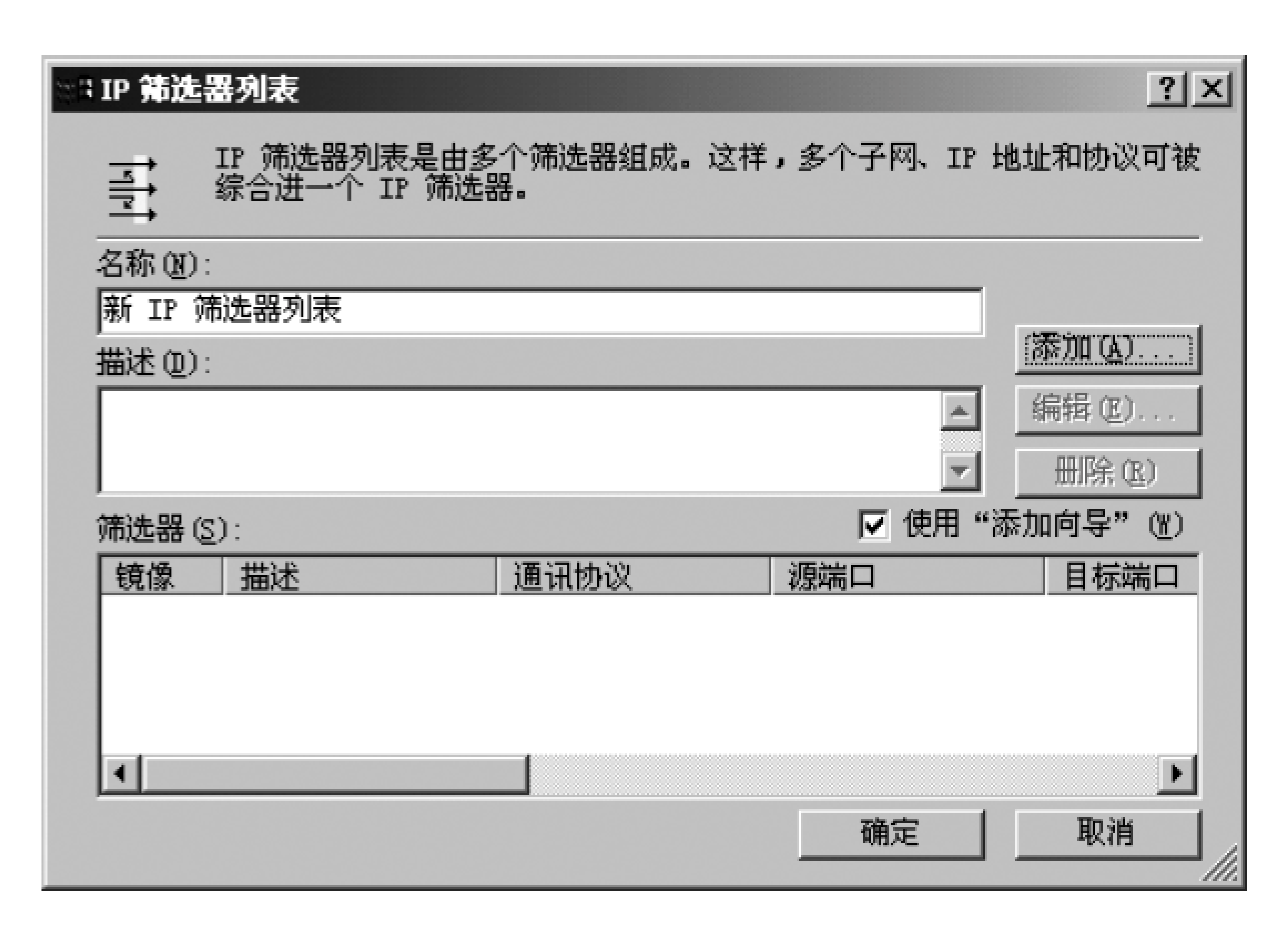


图 1.9 "IP 筛选器列表"页面

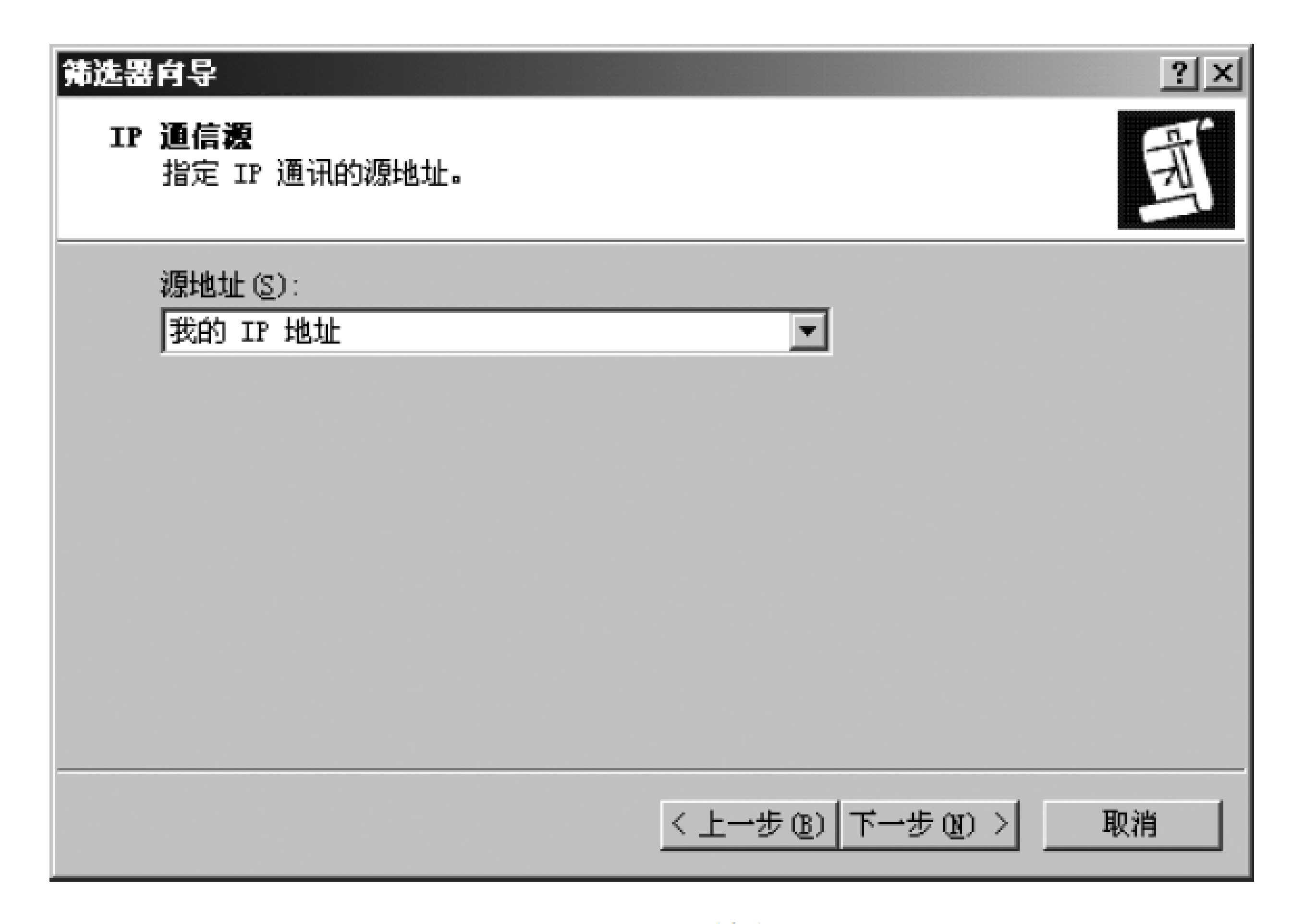


图 1.10 "IP 通信源"页面



图 1.11 "IP 通信目标"页面

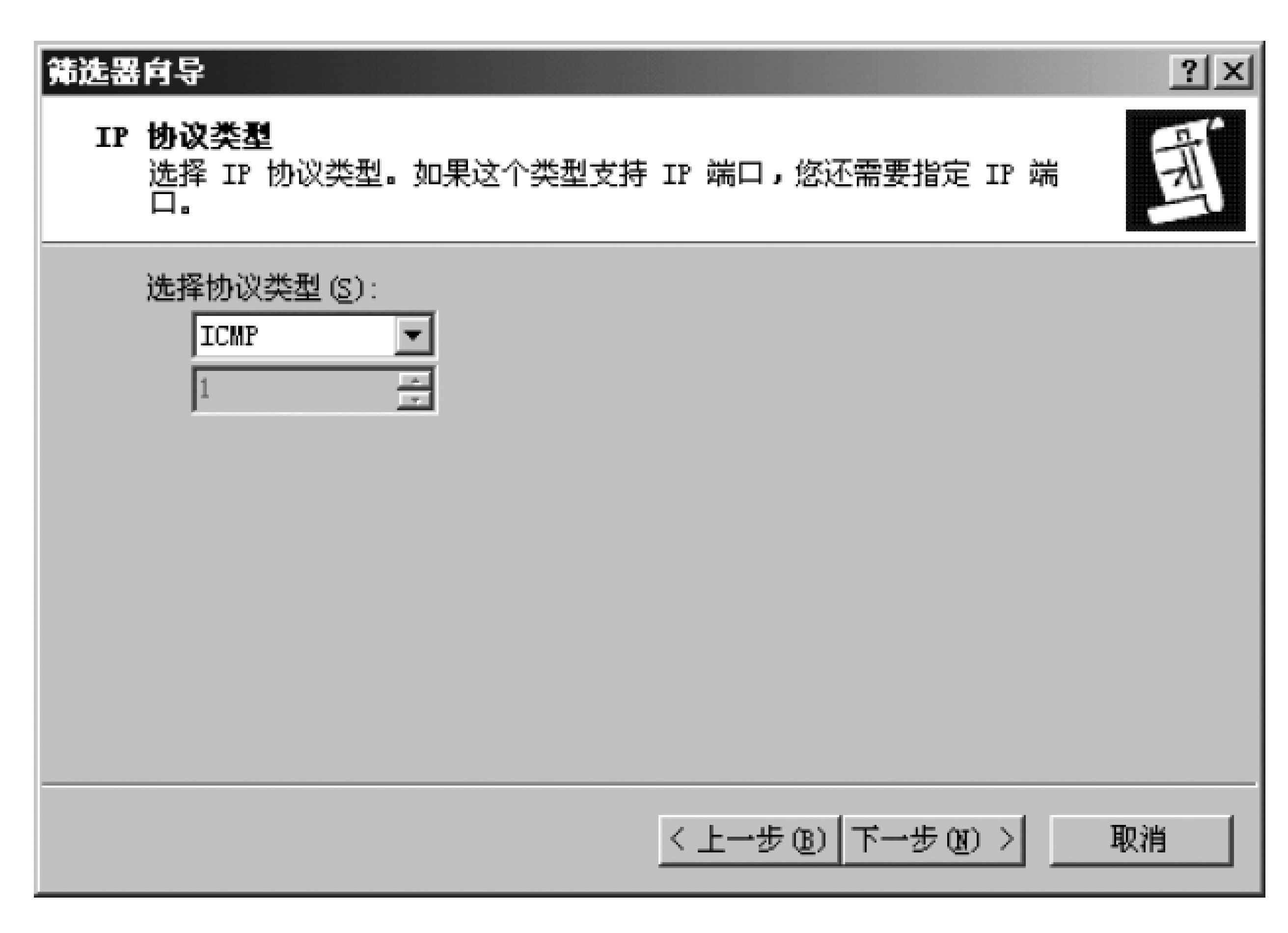


图 1.12　"IP 协议类型"页面

(9) 依次单击"下一步"、"完成"按钮，将在"IP 筛选器列表"对话框看到刚创建的筛选器，将其选中后单击"下一步"按钮，在出现的"筛选器操作"页面中设置筛选器操作为"要求安全设置"，如图 1.13 所示。

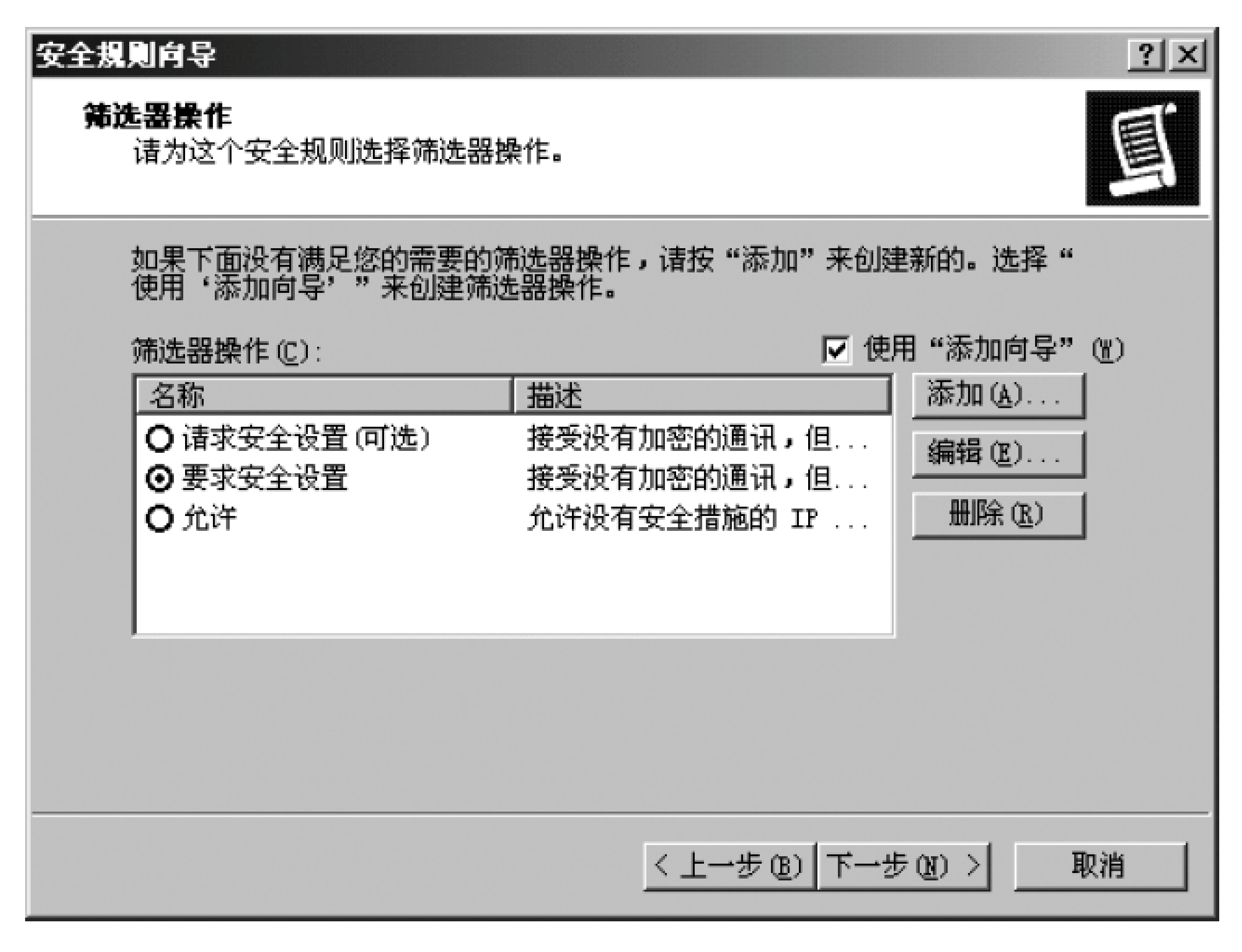


图 1.13　"筛选器操作"页面

(10) 单击"下一步"按钮，然后依次单击"完成"、"确定"、"关闭"按钮，保存相关的设置后返回控制台即可。

第 4 步　指派 IP 安全策略。安全策略创建完毕后并不能马上生效，还需通过"指派"功能令其发挥作用。方法是：在"控制台根节点"中右击"新 IP 安全策略"选项，在弹出的快捷菜单中选择"指派"命令，即可启用该策略，如图 1.14 所示。

至此，这台主机已经具备了拒绝其他任何机器 Ping 本机 IP 地址的功能，不过在本地仍然能够 Ping 通自己。经过这样的设置，所有用户(包括管理员)都不能在其他机器上对此服务器进行 Ping 操作，所以就不用担心被 Ping 操作攻击了。

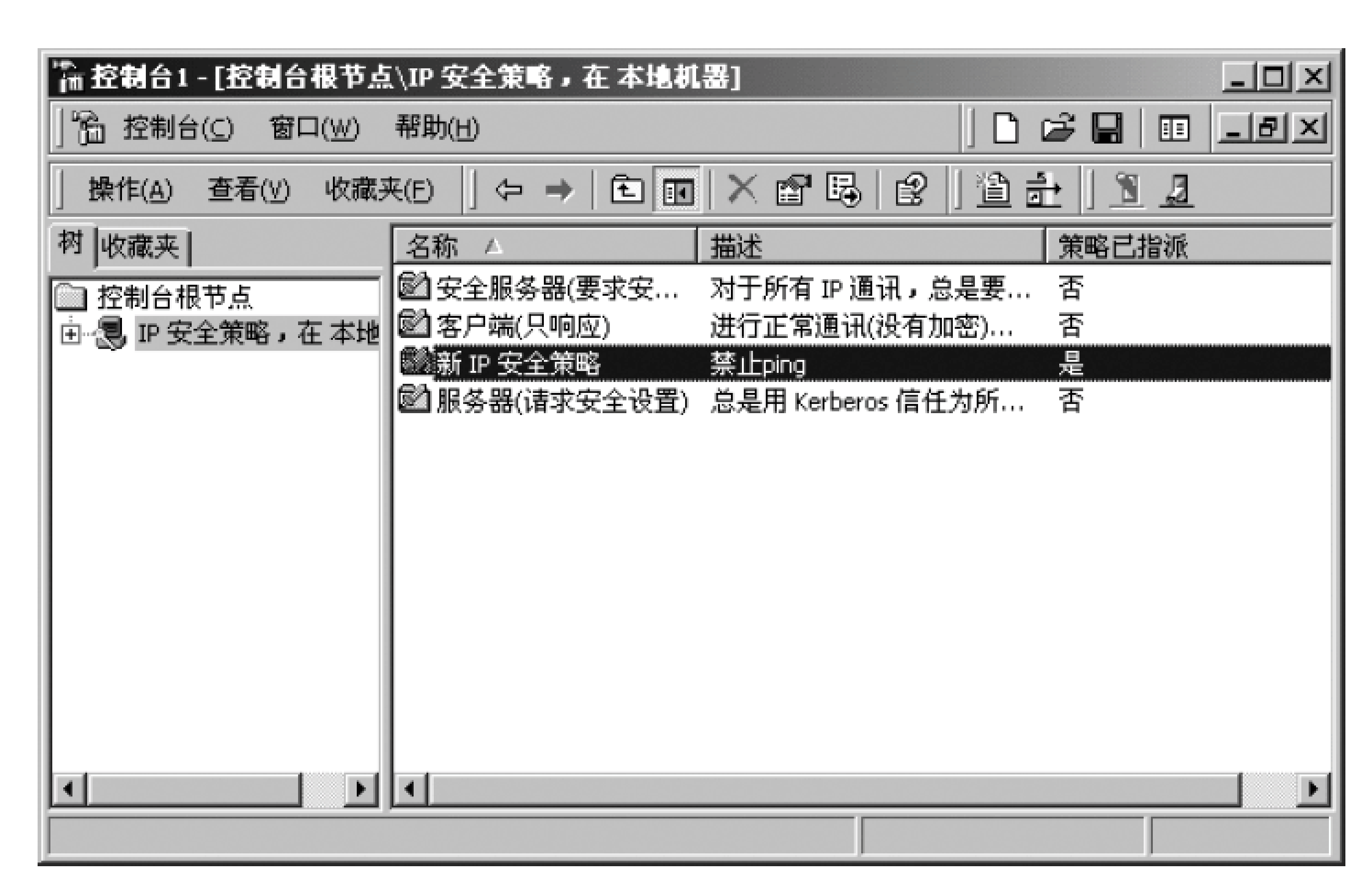


图 1.14　在“控制台根节点”中右击“新 IP 安全策略”选项

1.3　网络安全体系结构

网络安全体系的安全目标是系统的保密性、完整性与可用性的具体化。1989 年，为实现开放系统互联网环境下的信息安全，ISO/TC 97 国际标准化组织/技术委员会制定了 ISO 7498—2 国际标准。该标准从体系结构的观点描述了实现 OSI 参考模型之间的安全通信所必须提供的安全服务和安全机制，建立了开放系统互联标准的安全体系结构框架，为网络安全的研究奠定了基础。

1.3.1　安全服务

ISO 7498—2 提供以下 5 种可供选择的安全服务。

1. 鉴别

鉴别是访问控制的基础，是针对主动攻击的重要防御措施。鉴别服务包括两类：一是对等实体鉴别服务，这种服务是在两个开放系统(OSI)同等层中的实体建立连接和数据传送期间，为提供连接实体身份的鉴别而规定的一种服务，这种服务防止假冒或重放以前的连接，也即防止伪造连接初始化这种类型的攻击。这种鉴别服务可以是单向的，也可以是双向的。另一类是数据源鉴别服务，这是某一层向上一层提供的服务，它用来确保数据是由对等实体发出的，为上一层提供对数据源的对等实体进行鉴别，以防假冒。

2. 访问控制

访问控制的目的是控制不同用户对信息资源的访问权限，是针对越权使用资源的防御措施。访问控制可分为自主访问控制和强制访问控制两类。实现机制可以是基于访问控制的属性的访问控制表(或访问控制矩阵)，也可以是基于安全标签、用户分类及资源分档的多级控制。

3. 数据保密

数据保密服务的目的是保护网络中各系统之间交换的数据的安全，防止因数据被截获而造成的泄密，可分为如下几类。

(1) 连接保密。对某个连接上的所有用户数据提供保密。

(2) 无连接保密。对一个无连接的数据包的所有用户数据提供保密。

(3) 选择字段保密。对一个协议数据单元中的用户数据的一些经选择的字段提供保密。

4. 数据的完整性

数据的完整性是针对非法篡改信息而设置的防范措施，指的是防止网上传输的数据被修改、删除、插入、替换或重发，从而保护合法用户接收和使用该数据的真实性。

5. 防止否认

接收方要求发送方保证不能否认接收方收到的信息是发送方发出的信息，而非他人冒名、篡改过的信息；发送方也要求接收方不能否认已经收到的信息。防止否认是针对对方进行否认的防范措施，用来证实已经发生过的操作。

1.3.2 安全机制

为了实现上面各种安全服务，安全体系结构提出了如下 8 种安全机制。

1. 加密机制

加密是提供数据保密的最常用的方法。用加密的方法与其他技术相结合，可以提供数据的保密性和完整性。除了对话层不提供加密保护外，加密可在其他各层上进行。与加密机制伴随而来的是密钥管理机制。

2. 访问控制机制

访问控制根据实体的身份及其有关信息来决定该实体的访问权限。它可以防止未经授权的用户非法使用系统资源，这种服务不仅可以提供单个用户，也可以提供给用户组的所有用户。访问控制是通过对访问者的有关信息进行检查来限制或禁止访问者使用资源的技术。分为高层访问控制和低层访问控制。高层访问控制包括身份检查和权限确认，是通过对用户口令、用户权限、资源属性的检查和对比来实现的。低层访问控制是通过对通信协议中的某些特征信息的识别和判断来禁止或允许用户访问的措施，如在路由器上设置过滤规则进行包过滤就属于低层访问控制。

3. 数据完整性机制

数据完整性机制包括两个方面，即数据单元的完整性和数据序列的完整性。

数据单元的完整性是指组成一个单元的一段数据不被破坏和增/删篡改。通常是把

包含数字签名的文件用 Hash 函数产生一个标记,接收者在收到文件后也用相同的 Hash 函数处理一遍,看看产生的标记是否相同就可知道数据是否完整。

数据序列的完整性是指发出的数据分割为按序列号编排的许多单元,在接收时还能按原来的序列把数据串联起来,而不会发生数据单元丢失、重复、乱序、假冒等情况。

4. 数字签名机制

数字签名机制是以交换信息的方式来确认对象身份的方法,主要解决以下安全问题。

(1) 否认。发送者事后不承认自己发送过接收者提供的文件。

(2) 伪造。有人伪造了一份文件,却声称是某人发送的。

(3) 冒充。冒充别人的身份在网上发送文件。

(4) 篡改。接收者对收到的信息进行部分篡改,破坏原意。

数字签名机制具有可证实性、不可否认性、不可伪造性和不可重用性。

5. 交换鉴别机制

交换鉴别机制通过互相交换信息的方式来确定彼此的身份。常用的交换鉴别技术有以下几种。

(1) 口令。由发送方给自己的口令,以证明自己的身份,接收方则根据口令来判断对方的身份。

(2) 密码技术。发送方和接收方各自掌握的密钥是成对的。接收方在收到已加密的信息时,通过自己掌握的密钥解密,能够确定信息的发送者是掌握了另一个密钥的那个人。在许多情况下,密码技术还和时间标记、同步时钟、双方或多方握手协议、数字签名、第三方公证等相结合,以提供更加完善的身份鉴别。

(3) 特征实物。如 IC 卡、指纹、声音频谱等。

6. 公证机制

在一个大型网络中,使用这个网络的所有用户并不都是诚实可信的,同时也可能由于系统故障等原因使传输中的信息丢失、迟到等,这很可能引起区分责任承担者的问题。解决这个问题就需要有一个各方都信任的实体——公证机构,以提供公证服务,仲裁出现的问题。一旦引入公证机制,通信双方进行数据通信时必须经过这个机构来转换,以确保公证机构能得到必要的信息,供以后仲裁所需。

7. 业务流量填充机制

业务流量填充机制主要是对抗非法者在线路上监听数据并对其进行流量和流向分析。攻击者有时能够根据数据交换的出现/消失、数量或频率而提取有用的信息。数据交换量的突然改变也可能泄露有用信息。例如,当公司开始出售它在股票市场上的份额时,在消息公开前的准备阶段,公司可能与银行有大量通信。因此,对购买该股票感兴趣的人就可以密切关注公司与银行之间的数据流量以了解是否可以购买。

流量填充机制能够保持流量基本恒定,因此,观测者不能获取任何信息。流量填充的实现方法是:随机生成数据并对其进行加密,再通过网络发送。

8. 路由控制机制

路由控制机制可根据信息发送者的申请选择安全路径。这样,可以选择那些可信的网络节点,从而确保数据不会暴露在安全攻击之下。而且,如果数据进入某个没有正确安全标志的专用网络时,网络管理员可以选择拒绝该数据包。

1.4　计算机网络系统的安全评估

计算机网络系统的安全评估是对系统安全性的检验和监督。系统安全评估包括构成计算机系统的物理网络和系统的运行过程、系统提供的服务及这种过程与服务中的管理、保证能力的安全评估,一般来说包括如下几个方面。

(1) 明确该系统的薄弱环节。

(2) 分析利用这些薄弱环节实施威胁的可能性。

(3) 评估如果每种威胁都成功所带来的后果。

(4) 估计每种攻击的代价。

(5) 估算出将采取的应对措施的费用。

(6) 选取恰当的安全机制。

计算机系统的安全评估可以确保系统连续正常运行,确保信息的完整性和可靠性,及时发现系统存在的薄弱环节,采取必要的措施,杜绝不安全因素。另外,有了安全评估并不意味着可以高枕无忧,因为要在技术上做到完全的安全保护是不可能的。所以,评估的目标应该是使攻击所花的代价足够高,从而把风险降低到可接受的程度。

由于计算机系统用途及应用范围的不断扩大,不同的环境对系统可靠性、安全性、保密性的要求各不相同,这就要求有一个定量或定性的安全评估标准。这样的标准是系统安全评估的依据,也是计算机软/硬件生产厂家衡量其产品是否符合系统安全要求的依据。它不仅有利于安全产品的规范化,同时也有利于保证产品安全的可信性、可更新性和可扩展性。这个安全评估标准的重要性在于以下几个方面。

(1) 用户可依据标准,选用符合自己应用安全级别的、评定了安全等级的计算机系统,然后在此基础上再采取安全措施。

(2) 一个计算机系统是建立在相应的操作系统之上的,离开操作系统的安全,也就无法保证整个计算机系统的安全。所以,软件生产厂商应该满足用户的需求,提供各种安全等级的操作系统。

(3) 建立系统中其他部件(如数据库系统、应用软件、计算机网络等)的安全评估标准,可以使它们配合并适应相应的操作系统,以实现更完善的安全性能。

基于上述原因,世界各国都先后制定了相应的计算机系统的安全评估标准。

1.4.1 计算机网络系统的安全标准

第一个有关信息技术安全评价的标准诞生于20世纪80年代的美国。1983年，美国国防部发布了“可信计算机评估标准”，简称桔皮书。1985年对此标准进行了修订，之后作为美国国防部的标准。20世纪90年代，由于Internet技术的广泛应用，面对计算机系统安全出现的许多新问题，美国又颁布了联邦评测标准（FC）草案，用以代替80年代颁布的桔皮书。此外，美国还与加拿大和欧洲联合研制了信息技术安全评价通用标准（CCITSE），简称为CC标准。该标准发布的目的是建立一个各国都能接受的通用安全评价准则。在欧洲，英国、荷兰和法国带头联合研制欧洲共同的安全评测标准，并于1991年颁布ITSEC（信息技术安全标准）。1993年，加拿大发布加拿大可信计算机产品评估标准（CTCPEC）。在安全体系结构方面，ISO制定了国际标准ISO 7498—2—1989《信息处理系统　开放系统互联基本参考模型　第2部分：安全体系结构》。这些标准主要覆盖如下领域。

（1）加密标准。定义了加密的算法、加密的步骤和基本数学要求。目标是将公开数据转换为保密数据，在存储载体和公用网或专用网上使用，实现数据的隐私性和已授权人员的可读性。

（2）安全管理标准。它阐述的是安全策略、安全制度、安全守则和安全操作。旨在为一个机构提供用来制定安全标准、实施有效安全管理时的通用要素，并使跨机构的交易得以互信。

（3）安全协议标准。协议是一个有序的过程，协议的安全漏洞可以使认证和加密的作用前功尽弃。常用的安全协议有IP的安全协议、可移动通信的安全协议等。

（4）安全防护标准。它的内容包括防入侵、防病毒、防辐射、防干扰和物理隔离，也包括存取访问、远程调用、用户下载等方面。

（5）身份认证标准。身份认证是信息和网络安全的首关，它也同访问授权和访问权限相连。身份认证还包括数字签名标准、数字标准、眼睛识别标准等。

（6）数据验证标准。包括数据保密压缩、数字签名、数据正确性和完整性的验证。

（7）安全评价标准。其任务是提供安全服务与有关机制的一般描述，确定可以提供这些服务与机制的位置。

（8）安全审计标准。包括对涉及安全事件的记录、日志和审计，对攻击和违规事件的探测、记录、收集和控制。

1994年，国务院发布了《中华人民共和国计算机信息系统安全保护条例》，其中第九条规定：“计算机信息系统实行安全等级保护。安全等级的划分和安全等级保护的具体办法由公安部会同有关部门制定。”公安部在《中华人民共和国计算机信息系统安全保护条例》发布实施后便开始了计算机信息系统安全等级保护的研究和准备工作。等级管理的思想和方法具有科学、合理、规范，便于理解、掌握和运用等优点。因此，对计算机信息系统实行安全等级保护制度，是我国计算机信息系统安全保护工作的重要发展思想，对正在发展中的信息系统安全保护工作更有着十分重要的意义。

目前，计算机系统安全评价标准的一个发展趋势是建立最基本、稳定和经济的操作系

统评价标准，在此基础上再制定其他系统的安全评价标准。世界各国也正在为安全标准的完善进行广泛的接触和交流，并使其有了逐渐统一的趋势。

1.4.2 计算机网络系统的安全等级

常见的计算机系统安全等级的划分有两种：一种是美国国防部于1985年发表的评估计算机系统安全等级的桔皮书，将计算机系统的安全划分为4个等级、7个级别，即A、B3、B2、B1、C2、C1、D；另一种是依据我国颁布的《计算机信息系统安全保护等级划分准则》(GB 17859—1999)，该准则是计算机信息系统安全保护的法律基础，将计算机安全等级划分为5级，下面分别做出简要说明。

1. 美国颁布的桔皮书

(1) D级(非保护级)

这是可用的最低安全形式。该标准说明整个计算机系统是不可信任的，对于硬件来说，没有任何保护可用；操作系统很容易被侵袭。D级计算机系统标准规定对用户没有验证，也就是任何人都可以自由地使用该计算机系统。系统不要求用户进行登记(要求提供用户名)或口令保护(要求提供唯一的字符串来进行访问)。任何人都可以坐在计算机前使用它。D级的计算机系统包括MS-DOS、Windows 3.x、Windows 95，以及Apple的System 7.x。

(2) C1级

C1级也称自主安全保护系统，系统对硬件要求有某种程度的保护(如硬件带锁装置和需要钥匙才能使用计算机等)，用户必须登录到系统以便系统识别他们。C1级系统还要求具有完全访问控制的能力，应当允许系统管理员为一些程序或数据设立访问许可权限。C1级防护的不足之处在于用户可直接访问操作系统的根，不能阻止系统账户执行活动。常见的C1级兼容计算机系统如UNIX、XENIX、Novell 3.x或更高版本、Windows NT。

(3) C2级

C2级也称可控安全保护级，它解决C1级的某些不足之处并加强了几个安全特征。C2级具有进一步限制用户执行某些命令或访问某些文件的能力，这不仅基于许可权限，而且基于身份验证。对于一个C2系统的用户来说，使用附加身份验证，可以在没有根口令的情况下执行系统管理任务，这可以更好地完成追踪与系统管理有关的任务。

另外，这种安全级别要求对系统加以审核，包括为系统中发生的每个事件编写一个审核记录，以跟踪记录与安全有关的所有事件。常见的C2级操作系统有UNIX、XENIX、Novell 3.x或更高版本、Windows 2000。

(4) B1级

B1级也称标记安全保护级系统，支持多级安全，多级是指这一安全保护安装在不同级别的系统中(网络、应用程序、工作站等)，它对敏感信息提供更高级的保护，如安全级别可以分为解密、保密和绝密级别。

(5) B2级

B2级也称结构化的保护。B2级安全要求计算机系统中所有对象加标签，而且给设

备(如工作站、终端和磁盘驱动器)分配安全级别。如用户可以访问一台工作站,但可能不允许访问含有重要资料的子系统。

(6) B3 级

B3 级也称强制安全区域级,系统使用安装硬件的办法来加强域,如内存管理硬件用于保护安全域免受无授权的访问或其他安全域对象的修改。该级别也要求用户终端通过一条可信任途径连接到系统上。其主要特征是高抗渗透能力,可信恢复用于绝密、机密信息的保护,即使系统崩溃,信息也不会泄密。

(7) A 级

A 级也称验证设计级,是桔皮书中的最高安全级别。A 级除了包括其下面各级的所有特性,还有一个安全系统受监视的设计要求,合格的安全个体必须分析并通过这一设计。另外,必须采用严格的形式化方法来证明该系统的安全性。在 A 级,所有构成系统的部件的来源必须保证安全,这些安全措施还必须担保在销售过程中这些部件不受损害。例如,在 A 级设置中,一个磁带驱动器从生产厂房直至计算机房都得到严密的跟踪。A 级安全系统用于绝密级信息的保护。

美国的计算机安全等级评估标准虽然非常盛行,但它只是着重规定了某些操作系统的安全等级,而将之作为一个综合的评估标准还显得不完善。

2. 我国颁布的安全准则

从 2001 年 1 月 1 日起,我国实施强制性国家标准《计算机信息安全保护等级划分准则》。该准则是建立安全等级保护制度、实施安全等级管理的重要基础性标准。它将计算机信息系统安全保护划分为 5 个等级,从低到高依次如下。

(1) 用户自主保护级

本级的安全保护机制通过隔离用户与数据,使用户具备自主安全保护能力,从而保护用户和用户组信息,避免其他用户对数据的非法读写和破坏。

(2) 系统审计保护级

本级的安全保护机制除具备用户自主保护级的所有安全保护功能外,还要求创建和维护访问的审计跟踪记录,使所有用户对自己行为的合法性负责。

(3) 安全标记保护级

本级的安全保护机制有系统审计保护级的所有功能,并为访问者和访问对象指定安全标记,以访问对象标记的安全级别限制访问者的访问权限,实现对访问对象的强制保护。

(4) 结构化保护级

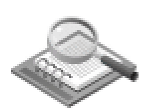
本级的安全保护机制具备安全标记保护级的所有安全功能,并将安全保护机制划分成关键部分和非关键部分相结合的结构,其中关键部分直接控制访问者对访问对象的存取。本级具有相当强的抗渗透能力。

(5) 访问验证保护级

本级的安全保护机制具备结构化保护级的所有功能,并特别增设访问验证功能,负责仲裁访问者对访问对象的所有访问活动。本级具有极强的抗渗透能力。

《计算机信息系统安全保护等级划分准则》就是要从安全整体上进行保护，从整体上、根本上、基础上来解决等级保护问题。要建立良好的国家整体保护制度，标准体系是基础。

《计算机信息系统安全保护等级划分准则》的配套标准分为两类：一是《计算机信息系统安全保护等级划分准则应用指南》，它包括技术指南、建设指南和管理指南；二是《计算机信息系统安全保护等级评估标准》，它包括安全操作系统、安全数据库、网关、防火墙、路由器和身份认证管理等。目前，国家正在组织有关单位完善信息系统安全保护制度的标准。



【案例】 使用扫描工具X-Scan检测系统漏洞

案例分析

利用扫描工具可以对计算机系统进行安全漏洞扫描，通过扫描结果对计算机系统的安全性进行评估，并采取相应的安全技术和管理措施。

操作环境

(1) 连上Internet的主机或局域网主机。
(2) Windows XP/2003系统。
(3) X-Scan 3.3扫描器。

操作步骤

第1步　运行X-Scan主程序，即可打开其操作窗口，如图1.15所示。



图1.15　X-Scan主窗口

第 2 步 选择“设置”→“扫描参数”命令，打开“扫描参数”窗口，在“检测范围”模块的“指定 IP 范围”文本框中输入要检测的目标主机的域名或 IP 地址，也可以对多个 IP 地址进行检测(如输入“192.168.0.1-192.168.0.255”来对处于这个网段的所有主机进行检测)，如图 1.16 所示。



图 1.16 “扫描参数”窗口

第 3 步 在“全局设置”模块中，可以对要扫描的模块、端口等进行设置，“扫描模块”选项用于检测对方主机的一些服务和端口等情况，可以全部检测或只检测部分服务，如图 1.17 所示。“并发扫描”选项用于设置检测时的最大并发主机和并发线程的数量。“扫描报告”选项用于设置扫描结束所产生的报告文件名和类型。这里假设选择 HTML 类型，如图 1.18 所示。



图 1.17 扫描模块设置



图 1.18 扫描报告设置

在"其他设置"中可设置"跳过没有响应的主机"功能,如果对方禁止了 Ping 操作或防火墙的设置使其没有响应,则 X-Scan 将会自动跳过,接着检测下一台主机。如果选择了"无条件扫描"功能,则 X-Scan 将会对目标主机进行详细检测,得到的结果相对详细、准确,但扫描时间会延长,对单个主机进行扫描一般会采用这种方式。具体如图 1.19 所示。

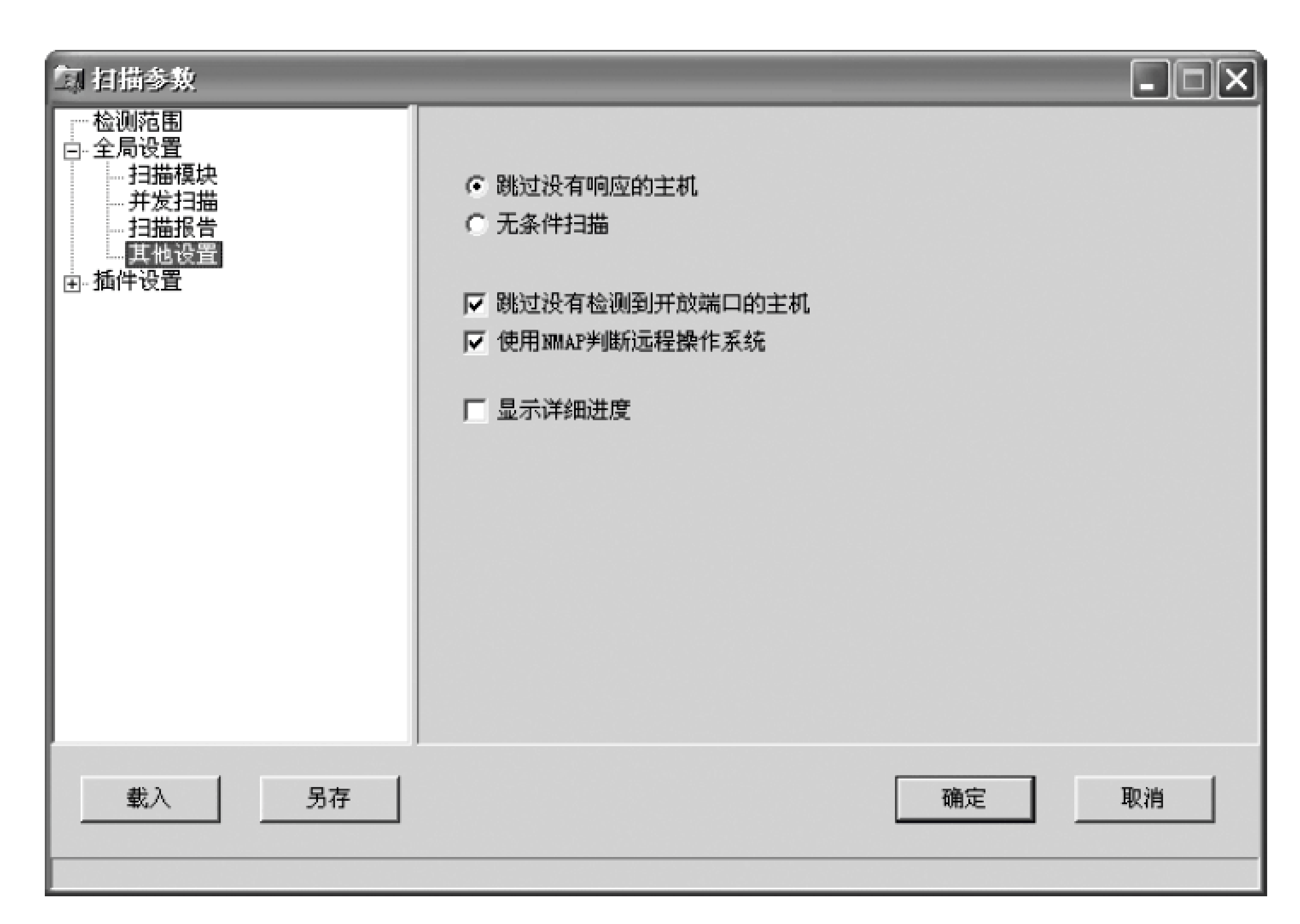


图 1.19 其他设置

第 4 步 在"插件设置"模块中,可以对插件进行一些必要的检测。

在"端口相关设置"中可自定义一些需要检测的端口,检测方式分 TCP 和 SYN 两种,TCP 方式容易被对方发现,但准确性要高一些;SYN 则相反,如图 1.20 所示。

"SNMP 相关设置"选项主要是针对 SNMP 信息的一些检测设置。"NETBIOS 相关设置"选项是针对 Windows 系统 NETBIOS 信息的检测设置,包括的项目有很多,只需要



图 1.20　端口相关设置

选择使用的内容即可。“漏洞检测脚本设置”、“CGI 相关设置”和“字典文件设置”等功能直接采用默认设置就可以了。

第 5 步　在设置好上述模块之后，返回 X-Scan主窗口中单击▷按钮，即可出现如图 1.21 所示的进度提示框。

正在加载漏洞检测脚本 ...

8%

取消

图 1.21　加载漏洞检测脚本提示框

第 6 步　漏洞检测脚本加载完毕就可以进行漏洞检测了，具体检测过程如图 1.22 所示。如果检测到漏洞，则可以在“漏洞信息”列表框查看。

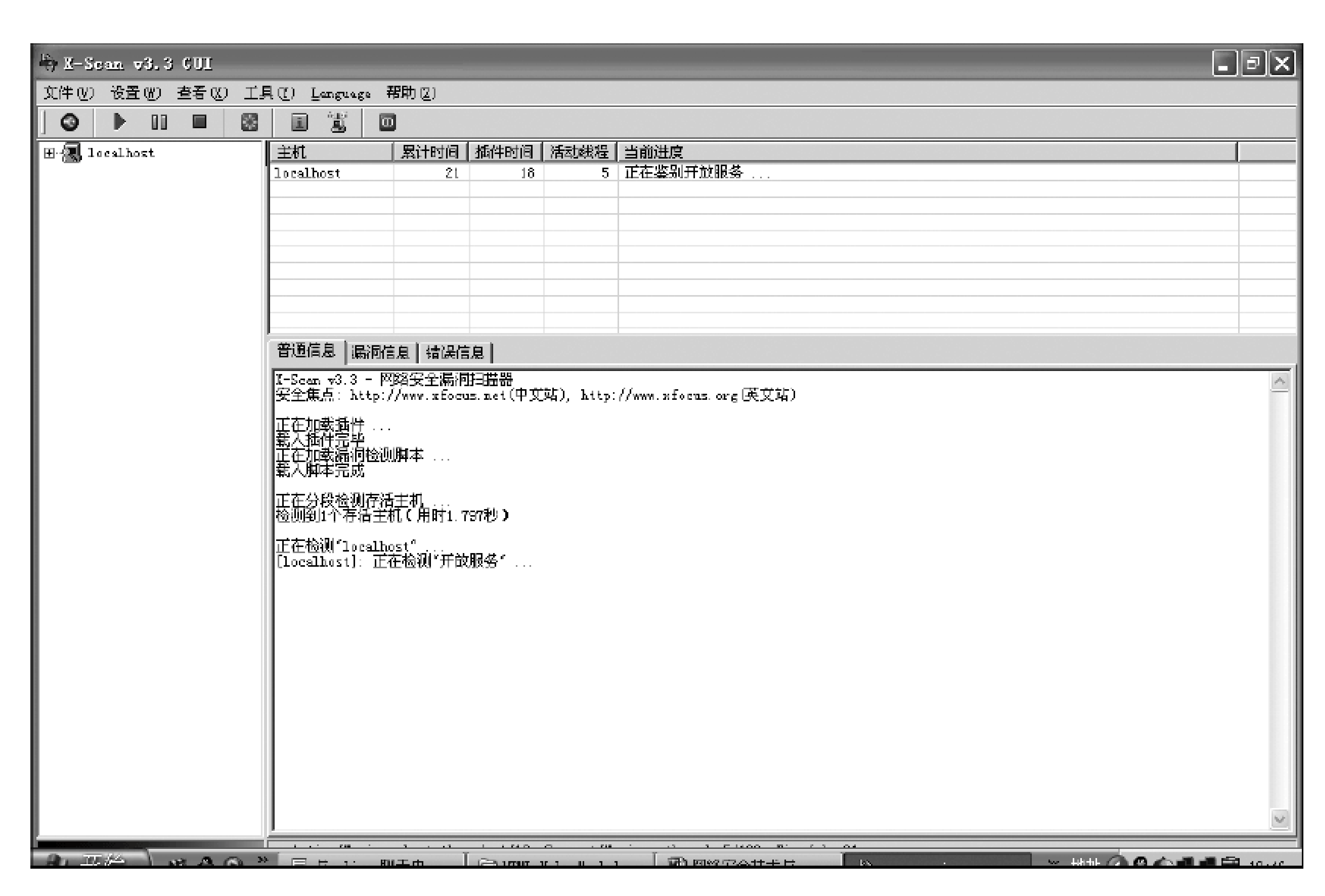


图 1.22　漏洞检测过程

第 7 步　扫描结束之后，将自动弹出检测报告，包括漏洞的风险级别和详细的信息，以便对所扫描的主机进行分析，如图 1.23 所示。

X-Scan 检测报告
本报表列出了被检测主机的详细漏洞信息，请根据提示信息或链接内容进行相应修补．欢迎参加X-Scan脚本翻译项目

扫描时间
2008-5-2 18:46:33 - 2008-5-2 18:52:31

检测结果	
存活主机	1
漏洞数量	0
警告数量	1
提示数量	15

主机列表	
主机	**检测结果**
localhost	发现安全警告
主机摘要 - OS: Windows XP; PORT/TCP: 25, 80, 110, 135, 445, 1025	

[返回顶部]

主机分析: localhost		
主机地址	**端口/服务**	**服务漏洞**
localhost	network blackjack (1025/tcp)	发现安全提示
localhost	microsoft-ds (445/tcp)	发现安全提示
localhost	http (80/tcp)	发现安全提示
localhost	pop3 (110/tcp)	发现安全提示
localhost	smtp (25/tcp)	发现安全提示
localhost	epmap (135/tcp)	发现安全提示
localhost	netbios-ssn (139/tcp)	发现安全警告

图 1.23　漏洞检测结果

本 章 小 结

计算机网络安全是指保持网络中的硬件、软件系统正常运行，使它们不因自然和人为的因素而被破坏、更改和泄露。网络受到的威胁来自于网络的内部和外部两个方面。

为实现开放系统互联网环境下的信息安全，ISO 7498—2 国际标准描述了实现 OSI 参考模型之间安全通信所必须提供的安全服务和安全机制。

计算机系统的安全评估是对系统安全性的检验和监督。在我国，常见的计算机系统安全等级的划分有两种：一种是依据美国国防部发表的评估计算机系统安全等级的桔皮书，将计算机安全等级划分为 4 个等级、7 个级别；另一种是我国颁布的《计算机信息系统安全保护等级划分准则》，将计算机安全等级划分为 5 级。

本 章 练 习

一、填空题

1. 一个安全的网络体系至少应包括三类措施，即________、________、________。
2. 网络安全主要包括________、________、________和运行安全等方面。
3. 一个安全的网络具有如下五个特征：________、________、________、________、________。

4. 网络的安全机制包括________、________、________、________、________、________、________和________。

5. 依据美国国防部发表的评估计算机系统安全等级的桔皮书，将计算机安全等级划分为________个等级________个级别。

二、选择题

1. 保护计算机网络设备免受环境事故的影响属于信息安全的________。
   A. 人员安全　B. 物理安全　C. 数据安全　D. 操作安全

2. 有些计算机系统的安全性不高，不对用户进行验证，这类系统安全级别是________。
   A. D1　B. A1　C. C1　D. C2

3. 保证数据的完整性就是________。
   A. 保证 Internet 上传送的数据信息不被第三方监视
   B. 保证 Internet 上传送的数据信息不被篡改
   C. 保证电子商务交易各方的真实身份
   D. 保证发送方不抵赖曾经发送过某数据信息

4. 某种网络安全威胁是通过非法手段取得对数据的使用权，并对数据进行恶意地添加和修改，这种安全威胁属于________。
   A. 窃听数据　B. 破坏数据完整性
   C. 拒绝服务　D. 物理安全威胁

5. 在网络安全中，捏造是指未授权的实体向系统中插入伪造的对象。这是对________。
   A. 可用性的攻击　B. 保密性的攻击
   C. 完整性的攻击　D. 真实性的攻击

三、简答题

1. 什么是网络安全？网络安全包括哪些方面？
2. 网络系统本身存在哪些安全漏洞？
3. 网络面临的威胁有哪些？
4. 怎样理解网络系统的脆弱性？
5. 网络的服务机制有哪些？安全机制有哪些？

实训　常用 DOS 命令操作

实训目的

掌握常用 DOS 命令的操作方法。

实训环境

（1）连上 Internet 的主机或局域网主机。

（2）Windows 2003/XP/2007 系统。

实训步骤

第 1 步　ping

功能：测试网络是否连通。

例 1　C:\>ping 192.168.10.243。

测试与主机 192.168.10.243 是否连通，如图 1.24 所示。

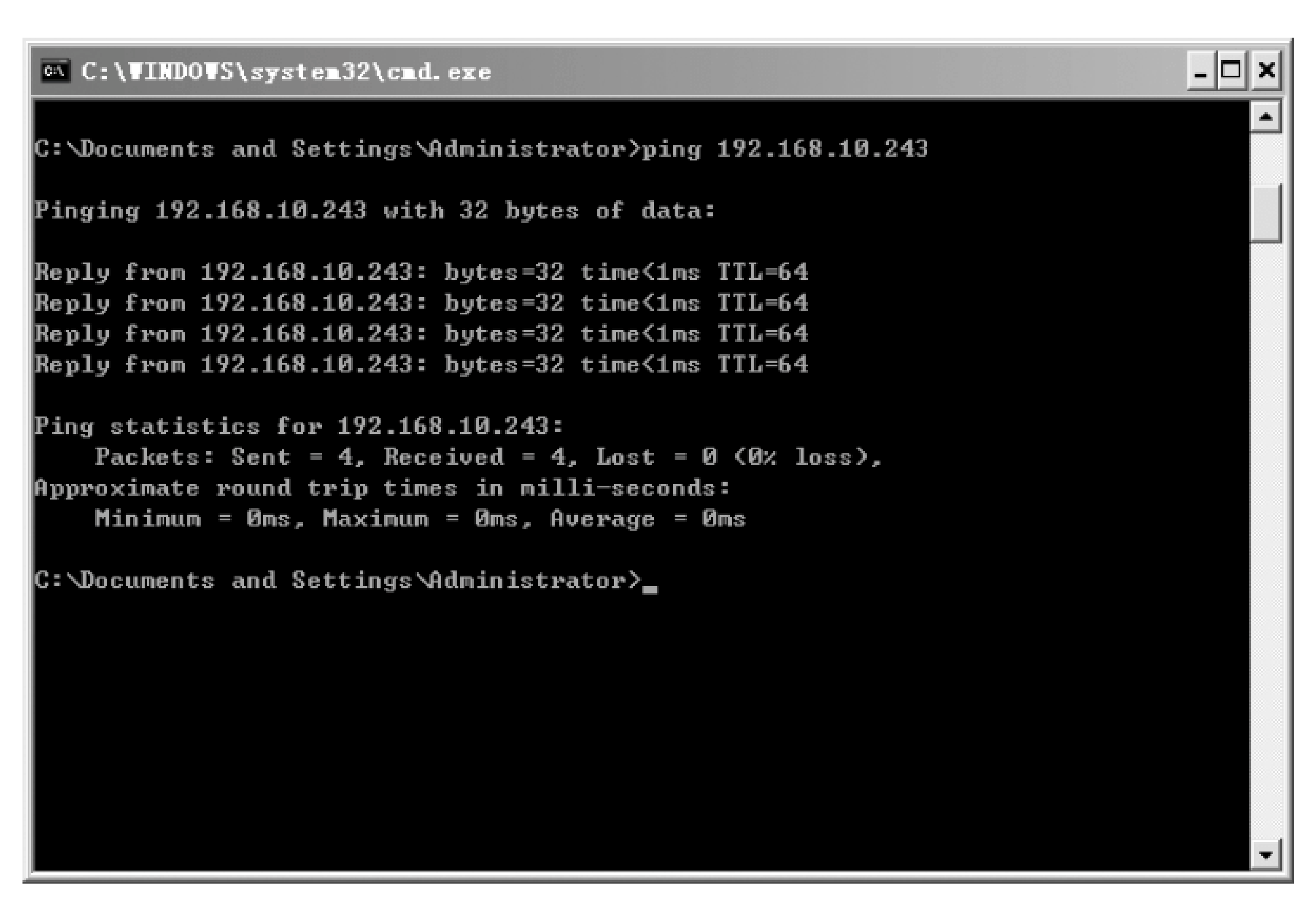


图 1.24　测试与主机 192.168.10.243 的连通性

第 2 步　ipconfig

功能：查看和修改网络中的 TCP/IP 协议的相关配置。

例 2　C:\>ipconfig。

查看当前主机 TCP/IP 协议的相关配置，如图 1.25 所示。

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . : domain
        IP Address. . . . . . . . . . . . : 192.168.1.108
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
```

图 1.25　查看当前主机 TCP/IP 协议的相关配置

第 3 步　dir

功能：列出当前路径下的文件目录。

例 3　C:\>dir。

列出 C 盘下的文件目录，如图 1.26 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\>dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 A882-E84E

 C:\ 的目录

2006-08-20  17:31    <DIR>          WINDOWS
2006-08-20  17:40    <DIR>          Documents and Settings
2006-08-20  17:59    <DIR>          Program Files
2006-08-20  18:00                 0 CONFIG.SYS
2006-08-20  18:00                 0 AUTOEXEC.BAT
2006-08-26  16:09    <DIR>          Drivers
2007-10-05  15:04    <DIR>          QQSG
2007-11-22  09:15         1,540,812 bsmain_runtime.log
2007-10-20  23:20    <DIR>          gfzq
2008-03-21  21:50               221 cmd.txt
2008-03-21  21:50                68 response.txt
2008-01-21  20:48    <DIR>          QQTang
2008-02-03  14:03           270,336 t39c.3
2008-05-02  18:47             1,024 .rnd
2008-03-03  19:48           270,336 t3c4
2008-03-05  20:46             4,096 t3r8.1
2008-05-04  12:28            91,210 BOOTEX.LOG
2008-04-05  13:33             1,200 error.txt
2008-05-04  14:31    <DIR>          内部帐目
2008-05-04  14:46                72 hack.bat
2007-08-30  13:37    <DIR>          jcb_cjscint
2007-08-30  13:41    <DIR>          dzh
2007-10-01  22:19            61,430 bsMain.txt
              13 个文件      2,240,805 字节
              10 个目录  7,231,455,232 可用字节

C:\>
```

图 1.26　列出文件目录

第 4 步　md

功能：在当前目录下建立文件夹。

例 4　C:\>md wangluo。

在 C 盘根目录下建立文件夹，如图 1.27 所示。

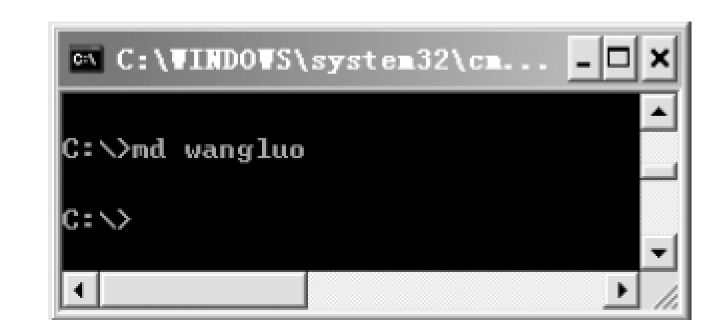


图 1.27　在 C 盘根目录下建立文件夹

第 5 步　echo

功能：文本建立命令。

例 5　建立一个内容如下，文件名为 1.txt 的文件，如图 1.28 所示。

你好！
我是中职的学生

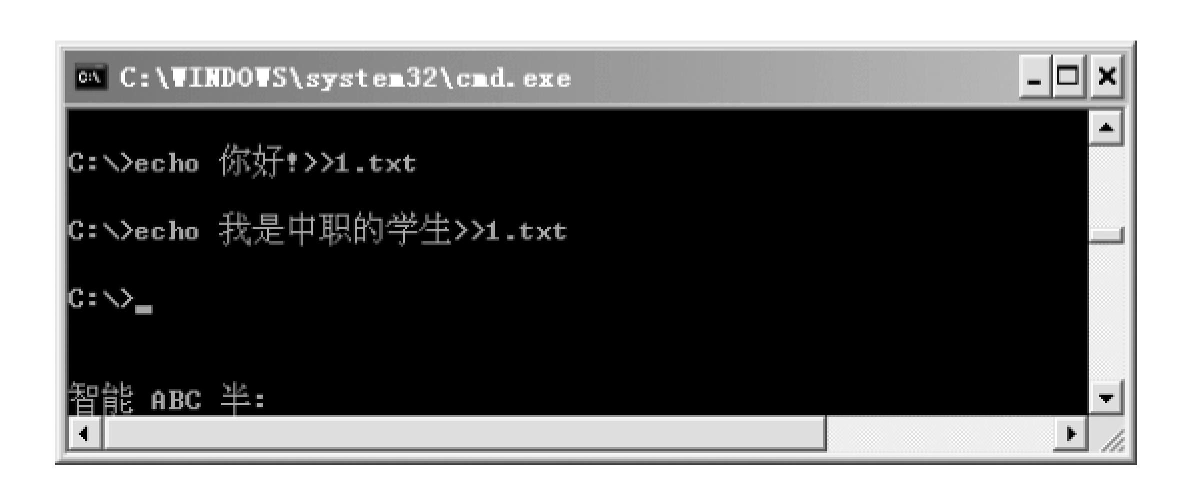


图 1.28　建立文件名为 1.txt 的文件

命令如下：

```
C:\>echo　你好!>>1.txt
C:\>echo　我是中职的学生>>1.txt
```

第6步　type

功能：显示指定文件的内容。

例6　C:\>type 1.txt。

显示1.txt文件的内容，如图1.29所示。

第7步　del

功能：删除指定文件。

例7　C:\>del 1.txt。

删除C盘的1.txt文件，如图1.30所示。

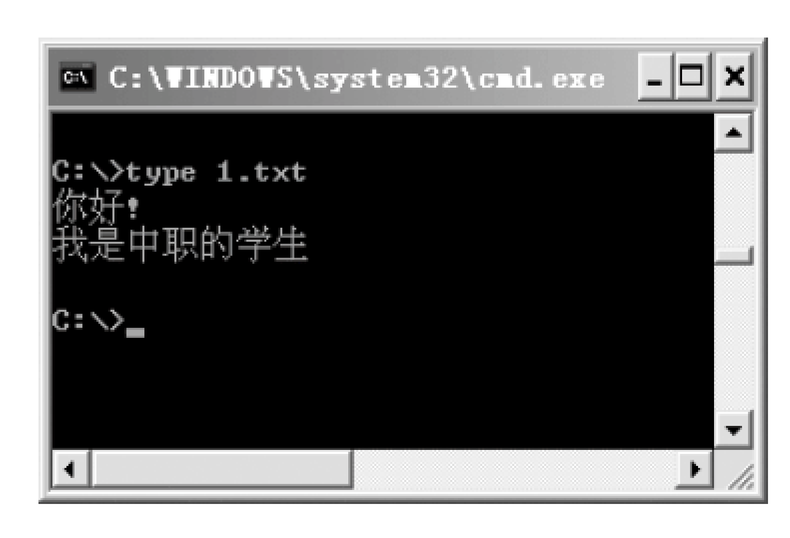


图1.29　显示1.txt文件的内容

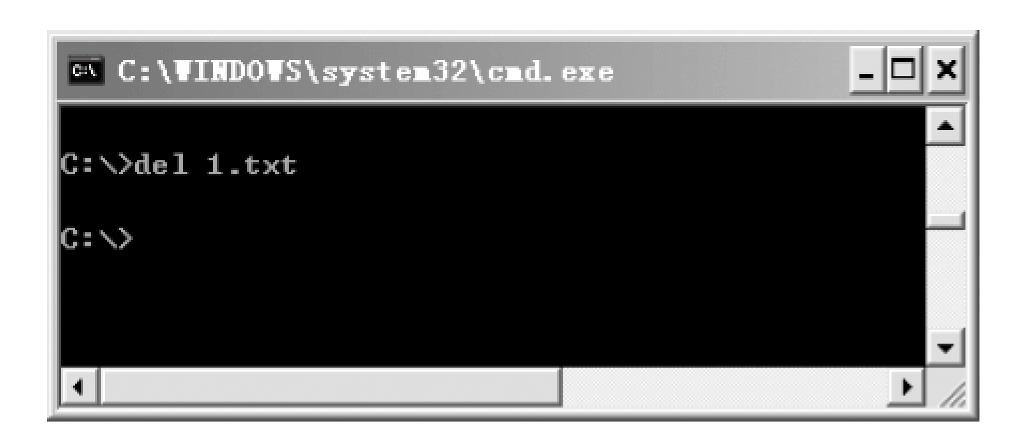


图1.30　删除C盘的1.txt文件

第8步　net

功能：管理网络环境、服务、用户及登录等本地信息的命令，后面加上相应的参数，就构成了相应的网络管理命令。

(1) net user

功能：系统账号管理。

例8　建立一个账号为1、密码为1的用户，如图1.31所示，该命令执行的结果如图1.32所示。



图1.31　建立一个账号为1、密码为1的用户

格式：

```
net user 用户名　密码 /add
net user 1　1 /add
```



图 1.32 net user 命令执行结果

(2) net stop“服务名”

功能：停止某系统服务。

例 9 net stop Telnet。

停止 Telnet 服务，如图 1.33 所示。



图 1.33 停止 Telnet 服务

(3) net start“服务名”

功能：启动某系统服务。

例 10 net start Telnet。

启动 Telnet 服务，如图 1.34 所示。



图 1.34 启动 Telnet 服务

(4) net config 命令

功能：显示当前运行的可配置服务或显示并修改某项服务的设置。

例 11 ① C:\net config 显示当前主机运行的可配置服务，如图 1.35 所示。

② C:\net config Workstation。

③ C:\net config Server。



图 1.35　显示当前主机运行的可配置服务

(5) net localgroup

功能：增加、显示、更改本地组。常用来提升本地用户权限。

例 12　C:\net localgroup　查看本地用户组。

例 13　C:\net use　查看本地用户。

例 14　C:\net localgroup administrators 1 /add。

将用户名为 1 的权限提升为管理员权限，如图 1.36 所示。



图 1.36　将用户名为 1 的权限提升为管理员权限

例 15　C:\ net localgroup administrators 1 /del。

(6) net share

功能：显示、创建及删除共享资源。

例 16　C:\>net share。

查看当前计算机中的共享资源，如图 1.37 所示。

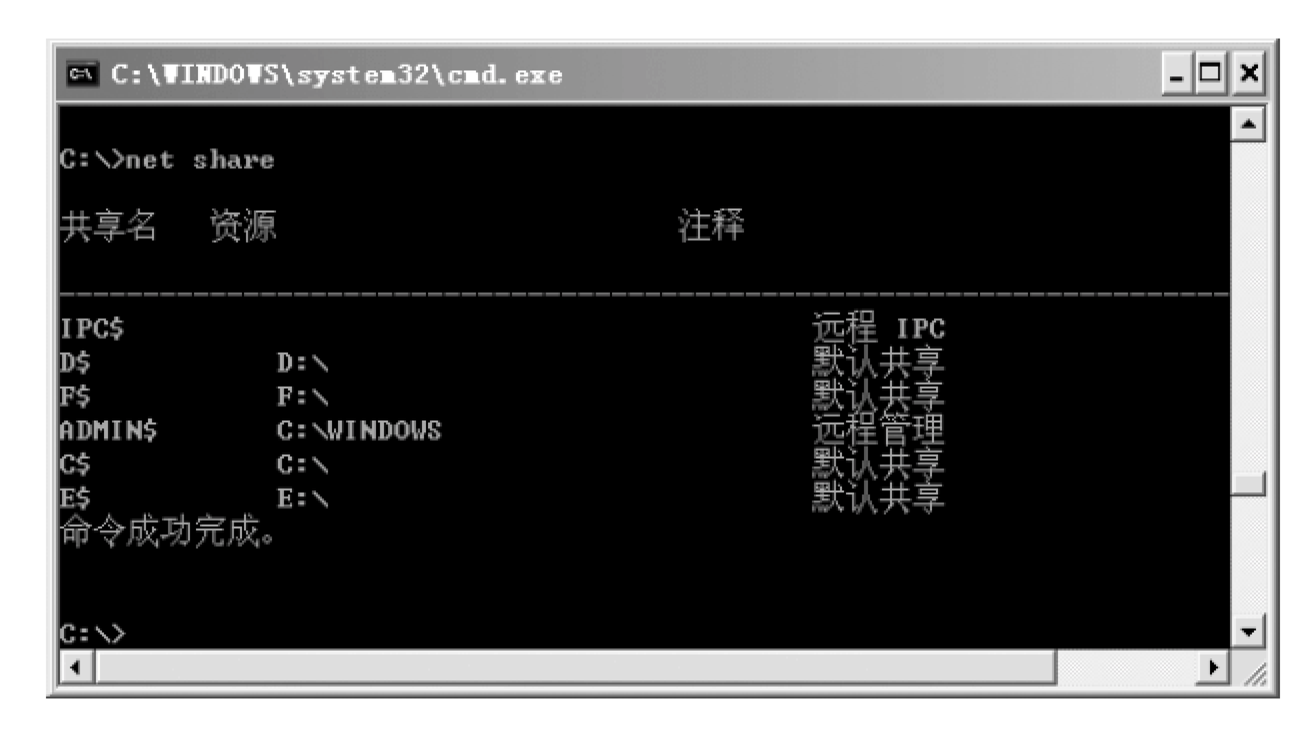


图 1.37　查看当前计算机中的共享资源

例 17　C:\>net share　s=D:\wanluo。

将 D 盘的 wanluo 文件夹共享为文件名称为 S 的共享文件夹。

(7) netstat　-an

功能：查看系统当前开放的端口和连接。

例 18　C:\>netstat　-an。

查看系统当前开放的端口和连接，如图 1.38 所示。

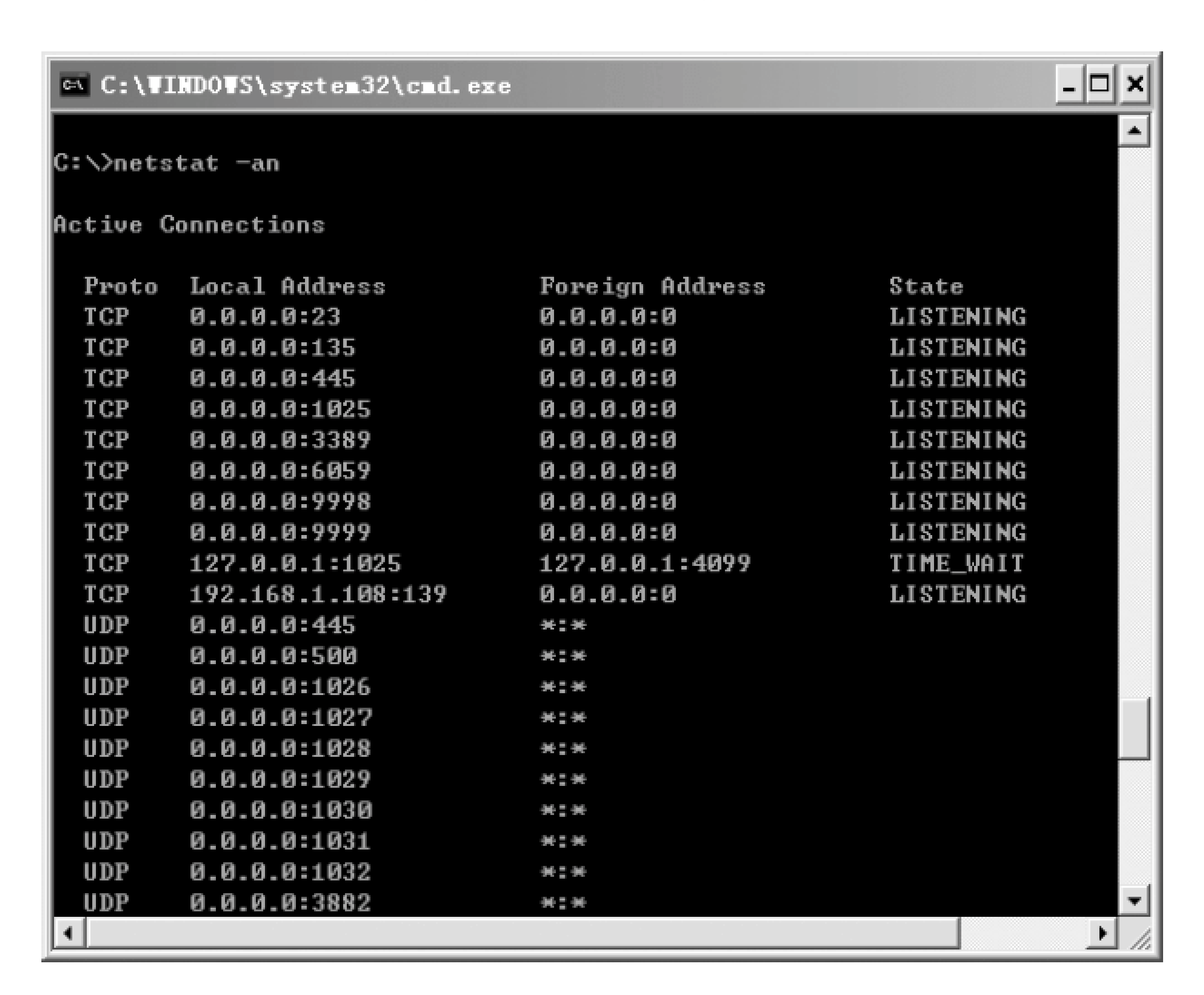


图 1.38　查看系统当前开放的端口和连接

(8) at

功能：在目标主机上添加计划任务，如图 1.39 所示。



图 1.39　在目标主机上添加一项计划服务

例 19　C:\>at　查看当前打开的计划。

例 20　C:\>at　\\192.168.0.70　20：50　D:\muma.exe　在指定的 IP 上添加一项计划服务。

例 21　C:\>at　\\192.168.0.70　查看 192.168.0.70 主机上的计划服务。

第2章
通信协议与安全

Chapter 2

知识目标

- 了解TCP/IP协议及其工作原理，了解以太网的工作原理。
- 掌握使网络通信不安全的因素，了解TCP/IP服务的脆弱性。
- 了解网络协议存在的安全问题。

技能目标

- 能够使用工具捕获、分析网络数据。
- 能够对通信协议采用相应的安全措施。

计算机网络的基础是网络通信协议。保证通信协议的安全对计算机网络的安全有重要的意义。

2.1 TCP/IP 协议

TCP/IP协议是先于OSI模型开发的，并不符合OSI标准。TCP/IP模型是于1974年首先定义的，而设计标准的制定则在20世纪80年代后期完成。TCP/IP实际上是由一组协议组成，是当前Internet使用的最流行的网络"标准"，虽然它并不是国际标准，但由于由它所构成的系统经过时间的考验，日臻成熟，基于这个协议的网上应用量大且面广，所以这些年来，它已经成为事实上的国际标准。

构成TCP/IP的协议有很多。传输层的TCP协议、网际互联层的IP协议和许多别的协议共同构成了TCP/IP协议族。其中最重要的两个核心协议是TCP协议与IP协议。

1. TCP/IP协议及其工作原理

TCP/IP协议由TCP协议和IP协议组成，它们是在Internet上的两个网络协议，分别叫作传输控制协议和互联网协议，属于众多TCP/IP协议族中的一部分。

TCP/IP协议族中的协议保证Internet上各种类型的计算机之间的数据传输，提供了几乎现在上网用到的包括电子邮件传输、文件传输、BBS、新闻组的发布及访问WWW的所有服务等。

(1) TCP/IP 协议的四层模型

从协议分层模型方面来看,TCP/IP 由 4 个层次组成,即网络接口层、网间网层、传输层和应用层,如图 2.1 所示。

HTTP SMTP INS FTP	SNMP RPC	应用层协议
TCP	UDP	传输层协议
IP ARP ICMP IGMP		网间网层协议
Ethernet	Token Ring	网络接口层协议

图 2.1 TCP/IP 协议的 4 层模型

① 网络接口层。网络接口层处于 TCP/IP 协议的最底层,负责接收 IP 数据报并通过网络发送,或者从网络上接收物理帧,抽出 IP 数据报,交给 IP 层。

② 网间网层。网间网层负责相邻计算机之间的通信,其功能包括:处理来自传输层的分组发送请求,收到请求后,将分组装入 IP 数据报,填充报头,选择去往目标机的路径,然后将数据报发往适当的网络接口;处理输入数据报,首先检查其合法性,然后进行寻径,假如该数据报已到达目标机,则去掉报头,将剩下部分交给适当的传输协议,假如该数据报尚未到达目标机,则转发该数据报;处理路径、流量控制、拥塞等问题。

③ 传输层。传输层提供应用程序间的通信,其功能主要是提供可靠传输。为实现后者,传输层协议规定接收端必须发回确认,并且假如分组丢失,则必须重新发送。

④ 应用层。应用层向用户提供一组常用的如电子邮件、文件传输访问、远程登录等应用程序。远程登录(Telnet)使用 Telnet 协议提供在网络其他主机上注册的接口。Telnet 会话提供了远程的虚拟终端。文件传输访问(FTP)使用 FTP 协议来提供网络内节点的文件拷贝功能。

(2) TCP/IP 协议的工作原理

TCP/IP 通过协议栈工作,这个栈是所有用来在两台计算机间完成一个传输的所有协议的几个集合。这也是一个通路,数据通过它从一台计算机传输到另一台计算机。数据在通过如图 2.1 所示的各个层后,就从网络的一台计算机传输到了另一台计算机。栈的每一层都能从相邻的层中接收或发送数据,每一层都与许多协议相联系。在栈的每一层,这些协议都在起作用。

(3) IP 地址

Internet 上的计算机和网络设备很多,在进行信息交换时必须先给每台计算机或网络设备取一个名字,称为 Internet 地址,即 IP 地址,它是用来表明网络上的每一台计算机或网络设备身份的地址,并且是唯一的。在 Internet 中,IP 地址不是任意分配的,它必须由相应的组织进行分配,如中国教育和科研计算机网(CERNET)的用户必须向 CERNET 网络管理中心申请 IP 地址。TCP/IP 协议对这个地址做了规定:一个 IP 地址由一个 32 位二进制数表示,共分为 4 组,每 8 位为一组,每组数字的取值范围为 0~255,相互之间用圆点(.)分隔,表示形式为×××.×××.×××.×××,如 192.168.0.100。一个 IP 地址由一个网络部分和一个主机部分组成,如图 2.2 所示。

网络地址部分	主机地址部分

图 2.2 IP 地址的格式

为了有效地利用地址空间，根据选择的网络地址和主机地址位数的不同对 IP 地址进行分类，IP 地址分为 A、B、C、D 和 E 五大类，最重要的是 A 类、B 类和 C 类 IP 地址。

通过 IP 地址的前三位，就能区分出 IP 地址是属于 A 类、B 类或 C 类，如 IP 地址的最高位为 0，则是 A 类 IP 地址，其第一字节的值为 0～127，A 类 IP 地址的主机容量为 16 777 216 台。B 类 IP 地址的最高两位为 10，其第一字节的值为 128～191，B 类 IP 地址的主机容量为 65 536 台。C 类 IP 地址的最高三位是 110，第一字节的值为 192～233，主机号只有 8 位，因此只能有 256 台主机。

将 IP 地址分成网络和主机部分，在路由寻址时非常有用，可以大大提高网络的速度。路由器(router)就是通过 IP 地址的网络号来决定是否发送数据包和将一个数据包发送到什么地方。

一个网络设备可以有多个 IP 地址，如连在两个物理网络上的路由器就有两个 IP 地址，分别连在两个不同的物理网络上，所以又可以将 IP 地址看成一个网络连接。网络上的代理服务器也可能使用两块网卡，配置两个属于不同网络的 IP 地址，或使用一块网卡配置两个属于不同网络的 IP 地址(如在 Windows NT 操作系统中)，即一个外部网络地址，一个内部网络地址。

2. 以太网

(1) 以太网的原理

局域网发展到今天，在实际应用中已相当普及。在各种局域网技术中，以太网(Ethernet)被广泛使用。

以太网是一种产生较早且使用相当广泛的局域网，以太网最早是由美国 Xerox(施乐)公司创建的，在 1980 年由 DEC、Intel 和 Xerox 三家公司联合提出了以太网规范，这是世界上第一个局域网的技术标准。后来的以太网国际标准 IEEE 802.3 就是参照以太网的技术标准建立的，两者基本兼容。为了与后来提出的快速以太网相区别，通常又将这种按 IEEE 802.3 规范生产的以太网产品简称为以太网。

几乎所有的以太网都遵从载波侦听多路访问/冲突检测(CSMA/CD)的通信规则。所有的以太网，不论其速度或帧类型是什么，都使用 CSMA/CD。以太网的存取方式是一种采用随机访问技术的竞争型(有冲突)的访问方法。因为多台计算机可以同时使用以太网，每台计算机根据是否有载波信号出现来判定总线是否空闲。如果主机接口有数据要传输，它就侦听，看总线上是否有信号在传输。如果没有探测到，它就开始传输。每次传输都在一定的时间间隔内，即传输的数据包有固定的大小。而且硬件还必须在两次传输之间，观察一个最小的空闲时间，也就是说，总线上的计算机使用通信线路的通信机会是均等的。

当开始一个传输时，信号并不能同时到达网络的所有地方，这就有可能两个设备同时探测到网络是空闲的，并都开始传输，当这两个信号在网络上相遇时，它们都不再可用了，这种情况就叫作冲突(collision)。

以太网在处理这种情况时，很有技巧性。每台设备在它传输信号的时候都监听总线，看它传输的时候是否有信号干扰，这种监视叫作冲突侦听，在探测到冲突后，设备就停止

传输。在以太网上，有可能会因为所有设备都忙于尝试传输数据而每次都产生冲突。

为了避免这种情况，以太网使用一个二进制后退策略。发送者在第一次冲突后，等待一个随机时间，再进行第二次传输，如果第二次还是冲突，则等待时间延长一倍，第三次再延长一倍，以此类推。通常这种策略，即使两台设备第二次等待的时间会很接近，但由于后面的等待时间成指数倍增长，不久，它们就不会冲突了。

(2) 以太网的帧地址

每台连接到以太网上的计算机都有一个唯一的 48 位(二进制数)以太网地址，以太网卡厂商都从一个机构购得一段地址，在生产时，给每块网卡一个唯一地址。通常，这个地址是固化在网卡上的，称为网卡的物理地址(MAC 地址)。

当一个数据帧到达时，硬件会对这些数据进行过滤，根据帧结构中的目的地址，将属于发送到本设备的数据传输给操作系统，而忽略其他任何数据。



【案例】 利用 Sniffer Portable 分析网络协议

案例分析

Sniffer 软件对网络管理员来说是一种强大的监控管理工具，可以分析网络中的协议、了解网络流量、发现异常通信等。对网络黑客而言它是一种重要的刺探工具，常用来窃取网络账号和密码，窃取网络通信或电子邮件信息。它是一把双刃剑，既为网络管理工作提供重要的信息资源，也为网络安全带来巨大的威胁。我们学习它的目的是为了把它更好地应用在网络管理中，同时对 Sniffer Portable 带来的网络安全威胁进行有效的预防。

Sniffer Portable 的主要功能如下。

(1) 捕获网络流量进行详细分析。

(2) 利用专家分析系统诊断问题。

(3) 实时监控网络活动。

(4) 收集网络利用率和错误等。

操作环境

(1) 局域网主机。

(2) Windows XP、Windows 7 系统，Sniffer Portable 软件。

操作步骤

第 1 步 Sniffer Portable 的启动。

Sniffer Portable 软件安装好后，选择"开始"→"所有程序"→Sniffer Pro→Sniffer 命令，启动 Sniffer Portable 程序，如图 2.3 所示。



图 2.3 启动 Sniffer Portable 程序

启动 Sniffer Portable 程序后首先出现的是 Settings 对话框，对话框中列表显示本计算机可以使用的各个网卡，若计算机中装有多个

网卡，需要从中选择准备用于监听的网卡，即选中与被监听系统连接的网卡，选中后单击“确定”按钮，如图 2.4 所示。

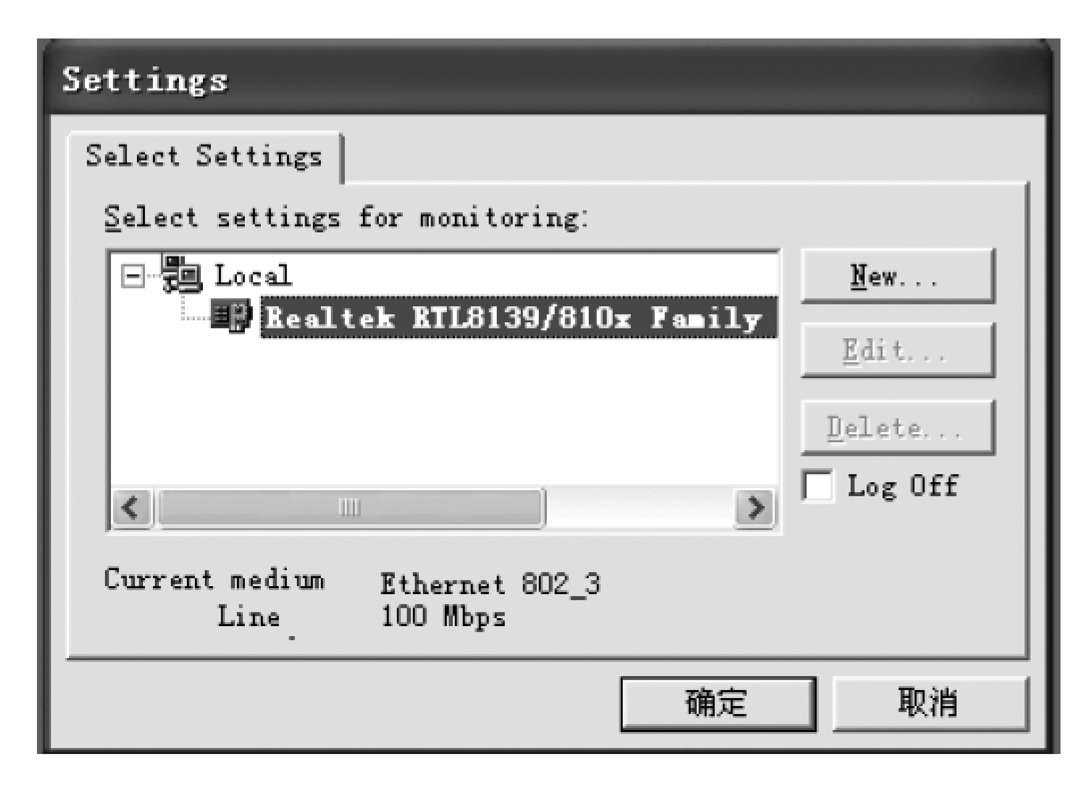


图 2.4　选中与被监听系统连接的网卡

Sniffer Portable 将打开如图 2.5 所示的主窗口。

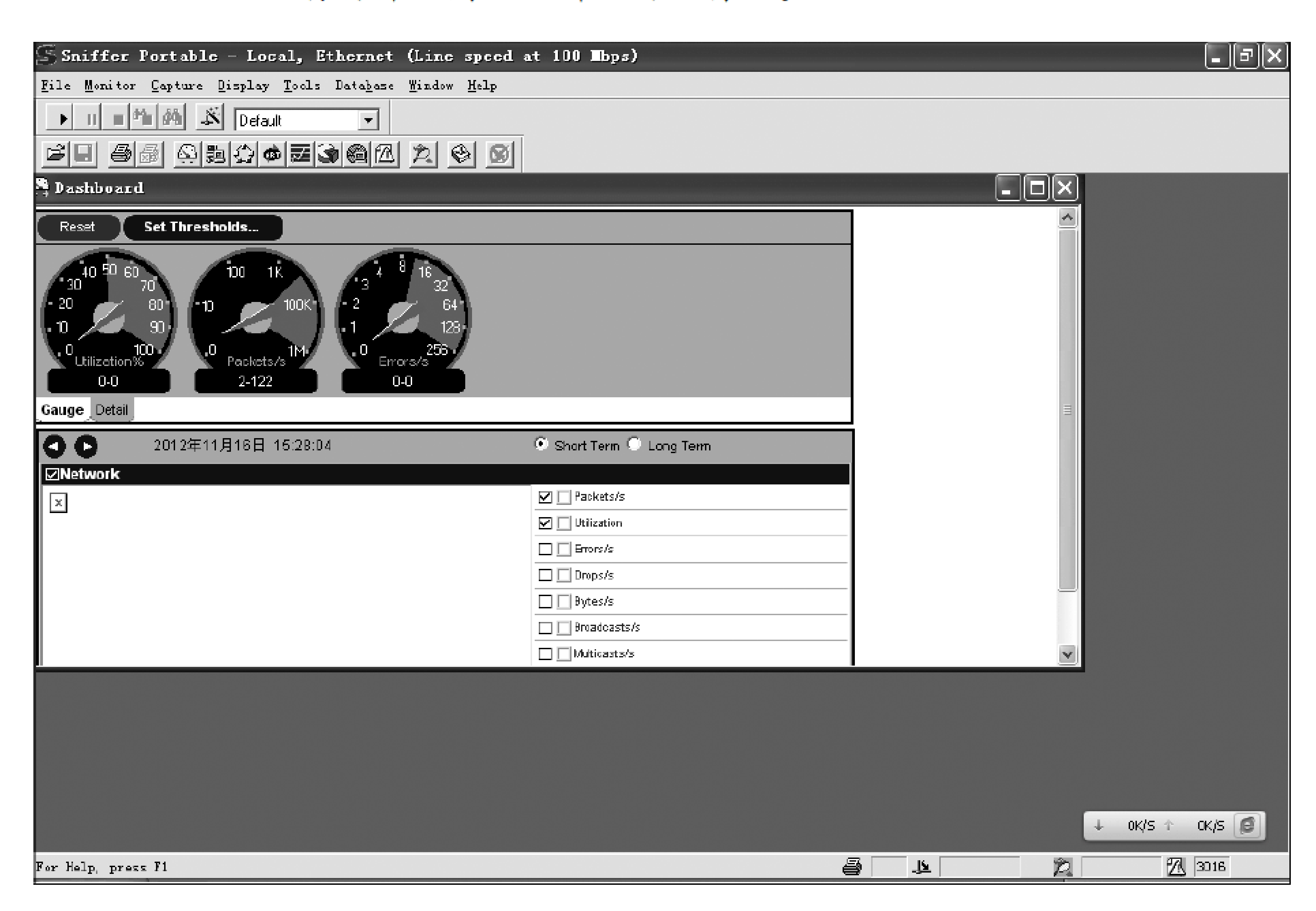


图 2.5　Sniffer Portable 主窗口

第 2 步　数据包的捕获。

捕获数据包需要将监听主机与被监听主机通过交换机连接在一起。Sniffer Portable 捕获工具栏共有 6 个按钮，如图 2.6 所示。6 个按钮的功能分别如下。



图 2.6　捕获工具栏按钮

- “开始”按钮：启动捕获程序，开始捕获数据包。
- “暂停”按钮：暂时停止捕获工作。
- “停止”按钮：停止捕获工作。
- “停止和显示”按钮：停止捕获工作，自动转到捕获数据包窗口。
- “显示”按钮：显示捕获数据包的内容。
- “定义过滤器”按钮：设置过滤条件，有选择地进行捕获。捕获方法很简单，单击捕获工具栏上的“开始”按钮即可开始捕获。

一旦捕获到有效数据包，捕获工具栏上的“停止和显示”按钮由灰色变为彩色，单击此按钮可以停止捕获并显示捕获数据包的内容，如图 2.7 所示。



图 2.7　显示捕获数据包的内容

第 3 步　数据包的读取与分析。

Sniffer Portable 捕获到的数据包被暂存在内存里，单击“显示”或“停止和显示”按钮可以把捕获的数据包内容显示出来。

在数据显示窗口中，通过窗口标签可以选择多种显示模式。

(1) 专家模式是一种综合显示模式，将各种捕获数据的信息综合排列显示在窗口中，如图 2.8 所示。

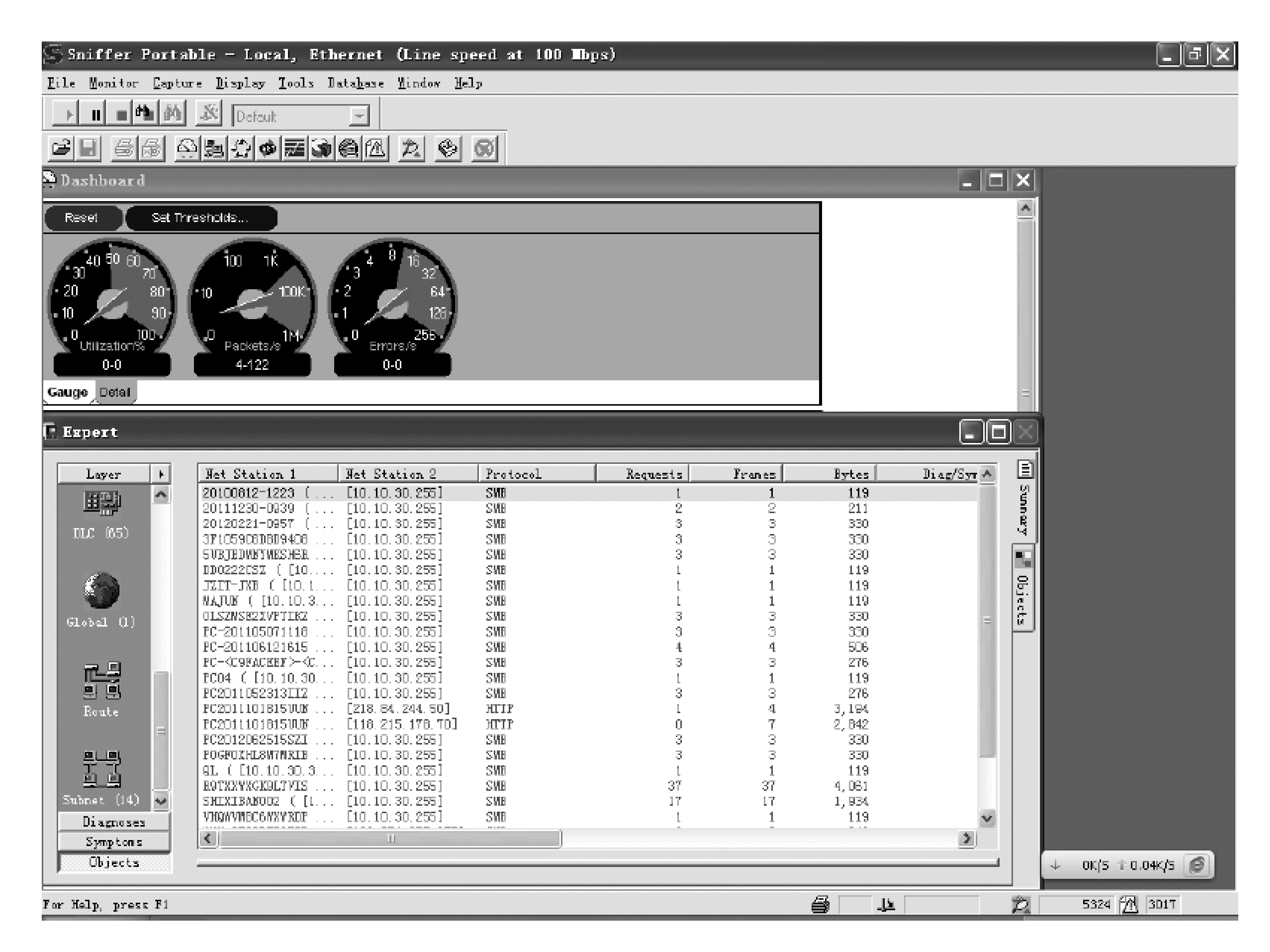


图 2.8　专家模式

(2) 矩阵显示模式可以直观地从捕获的数据包中看出哪些地址的主机间进行了何种协议的连接，如图 2.9 所示。

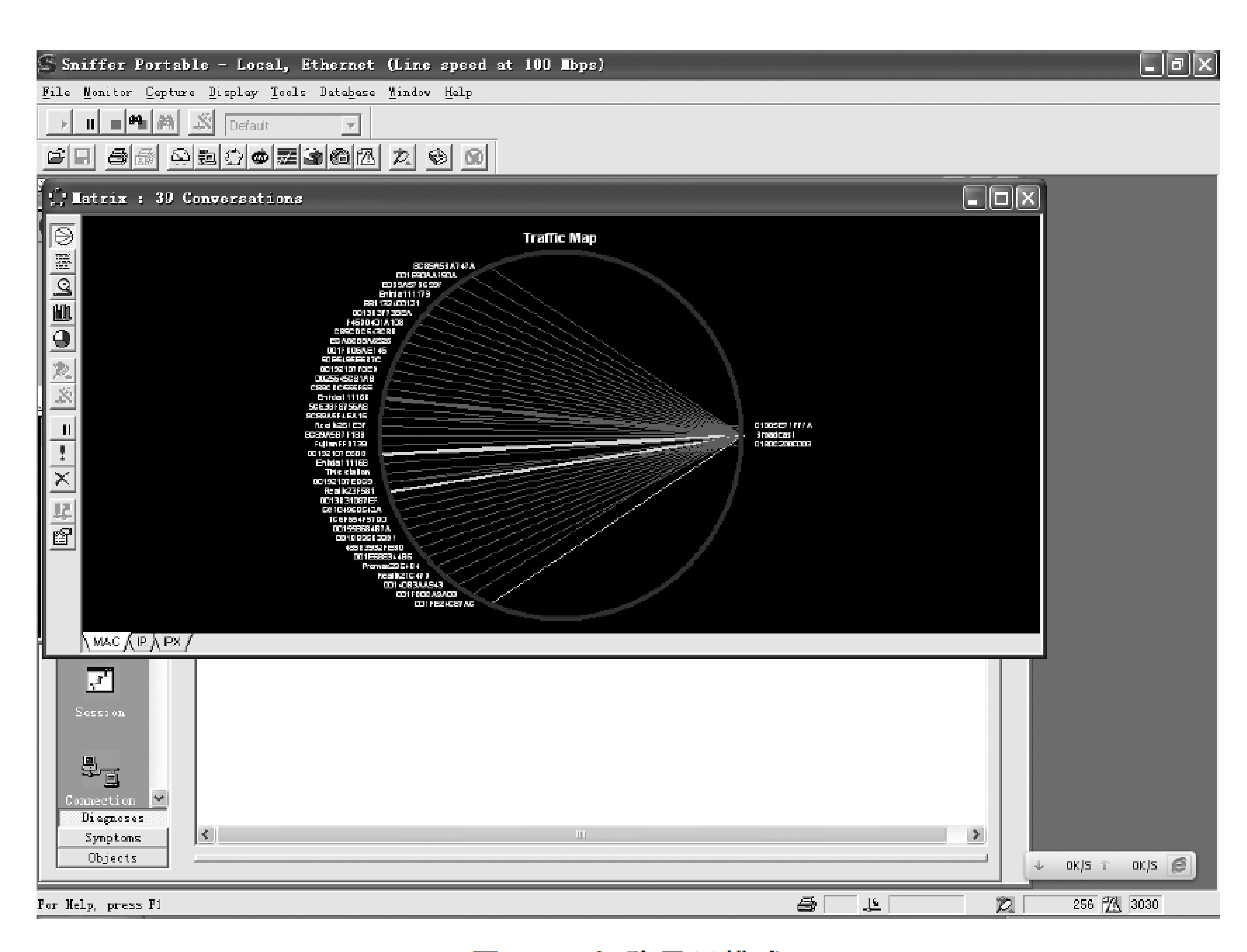


图 2.9 矩阵显示模式

(3) 主机列表显示模式详细列出每一个地址上各种协议出入数据包的数量及字节数,如图 2.10 所示。

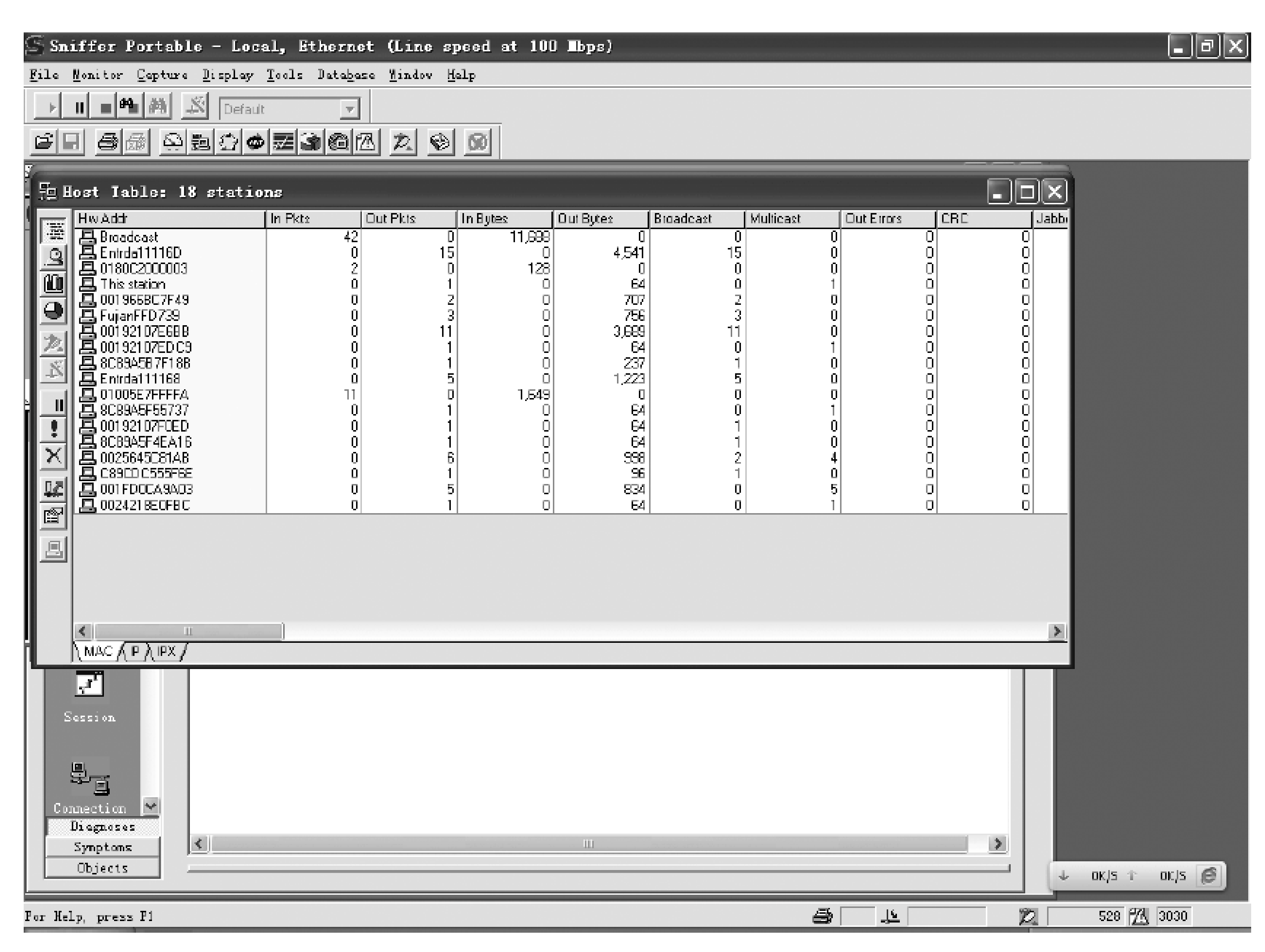


图 2.10 主机列表显示模式

第 4 步 捕获过滤。

Sniffer Portable 的信息捕获能力很强，在一瞬间可以捕获大量的数据，其中有些数据是有价值的，但绝大多数是无用的，如果不对这些数据进行有选择地捕获，会占用大量的系统资源，还会给有用信息的提取带来困难。

Sniffer Portable 有着很强的数据过滤功能，通过合理配置过滤器，可以仅对有价值的信息进行捕获，提高系统工作效率，降低系统工作负荷。

单击 Sniffer Portable 捕获工具栏上的“定义过滤器”按钮，可以打开 Define Filter－Monitor 对话框。在该对话框中可以设置按指定的地址及指定地址上的数据传输方向进行过滤，如图 2.11 所示。

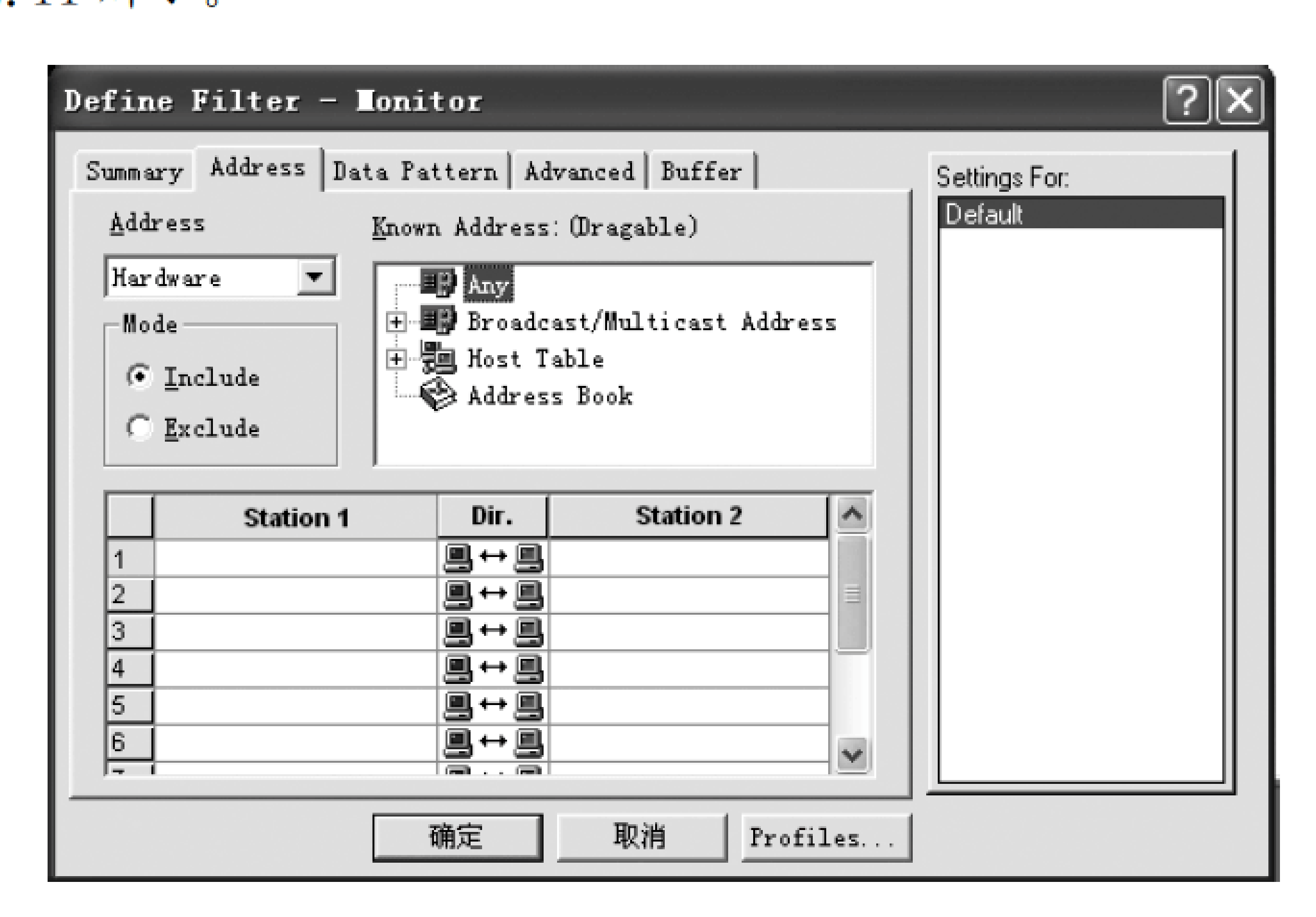


图 2.11 Define Filter－Monitor 对话框

也可以设置按某种协议或数据包大小进行捕获，如图 2.12 所示。

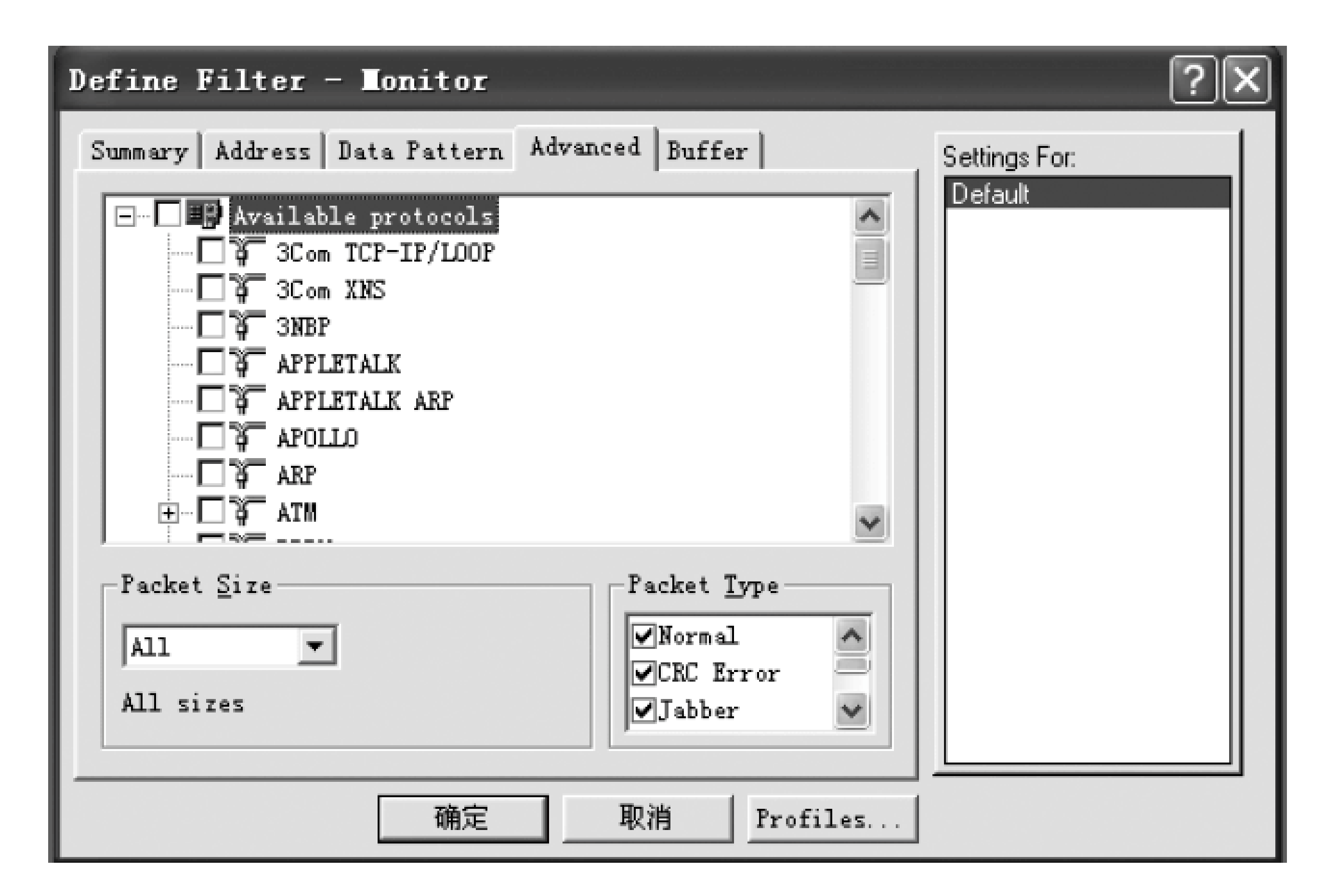


图 2.12 设置按某种协议或数据包大小进行捕获

可以设置捕获缓冲区的大小，及设置自动将缓冲区内容保存到指定位置的文件中，如图 2.13 所示。

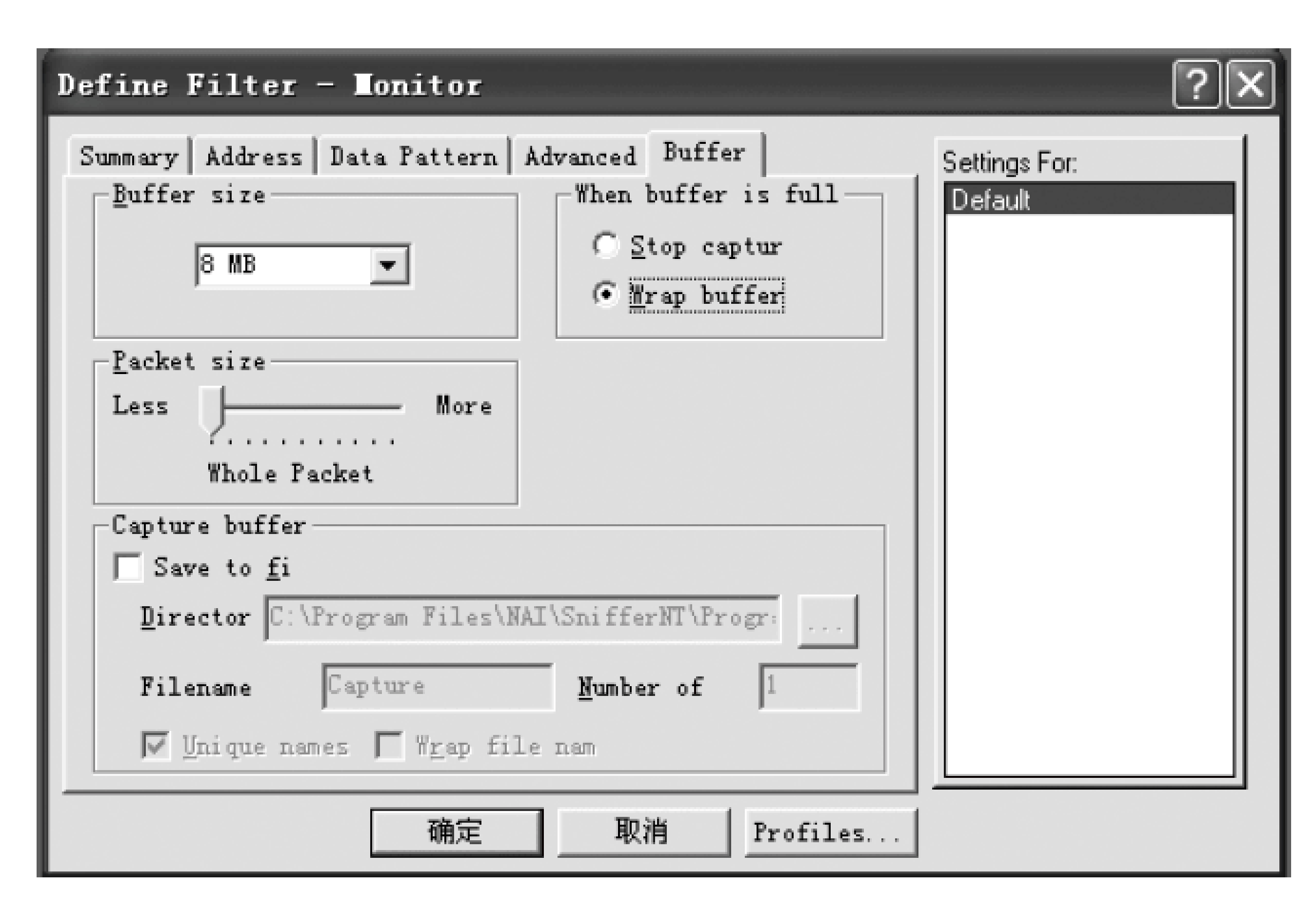


图 2.13 设置捕获缓冲区的大小

通过对上面这些过滤条件的指定，就可以有针对性地进行信息捕获，使捕获的数据都是所需要的信息。

2.2 网络通信不安全的因素

在生活中经常会看到或听到这样的消息：一个黑客入侵了某一网络，使该网络的服务器全部瘫痪；一个黑客利用网络从某一银行盗取了大量钱财，等等。这些例子说明 Internet 是不安全的，Internet 需要更多、更好的安全机制。事实上，世界上没有绝对安全的网络，只要用户的计算机网络连接到 Internet 上，它就存在着危险。安全问题的一个主要方面就是使用的 TCP/IP 协议本身就存在着巨大的安全缺陷，包括建立在其上面的很多服务。

221 网络自身的安全缺陷

Internet 的基石是 TCP/IP 协议，该协议在实现上力求简单、高效，而没有考虑安全因素，因为考虑安全因素，无疑会增大程序代码量，从而降低 TCP/IP 的运行效率，所以说 TCP/IP 协议本身在设计上就是不安全的，主要存在以下安全缺陷。

1. 容易被窃听

大多数 Internet 上的数据信息流量是没有加密的，电子邮件口令、文件传输等很容易被监听和劫持，可以实现这些行为的工具很多，在网上还有很多免费提供的工具。

2. 脆弱的 TCP/IP 服务

在 Internet 上，很多基于 TCP/IP 的应用服务都在不同程度上存在安全问题，这很容易被一些对 TCP/IP 协议十分了解的人所利用，尤其是一些新的处于测试阶段的服务有更多的安全缺陷。

3. TCP/IP 协议缺乏安全策略

由于技术水平的原因,Internet 上的许多网络站点在防火墙的配置上无意识地扩大了访问权限,忽视了这些权限可能会被网络内部的人利用或滥用,黑客从一些服务中可以获得有用的信息,而网络管理或维护人员却不知道应该禁止这种服务。

4. 配置的复杂性

在 Internet 上,访问控制的配置一般是很复杂的,所以很容易被错误配置或配置不完善,黑客便有了可乘之机。

222 网络容易被窃听和欺骗

由于局域网的特点使网络极易被窃听。Internet 是把无数局域网连接起来形成一个大网,然后再把大的网连接成更大的网,从而形成一个庞大的网络。它的拓扑结构是一种逐步细化的树状结构,虽然 Internet 上的信息传输是点对点的,但一般 Internet 的主机会处于一个特定的局域网中,例如,一个学校的一个计算机实验室构成了一个局域网,它连接到学校的校园网,校园网又连接到 CERNET,CERNET 又连接到国内的其他网络或直接连到国外的网络上。因为局域网,如以太网、令牌网等,都是广播型网络,也就是说,网络上的一台主机发布消息,网络上的任何一台机器都可以收到这个消息。一般情况下,以太网卡在收到发往别人的消息时会自动丢弃消息,而不向上层传递消息,但如果我们把以太网卡的接收模式设置成混合型(promiscuous)时,网卡就会捕捉所有的数据包,并把这些数据包向上传递,也就造成了以太网可以被窃听。其实,FDDI、令牌网等也存在这样的问题。现在的 ATM 网络技术是点对点的,它不会像以太网的广播型网络那样容易被窃听。图 2.14 描述了以太网卡混合工作方式和普通工作方式的工作原理。

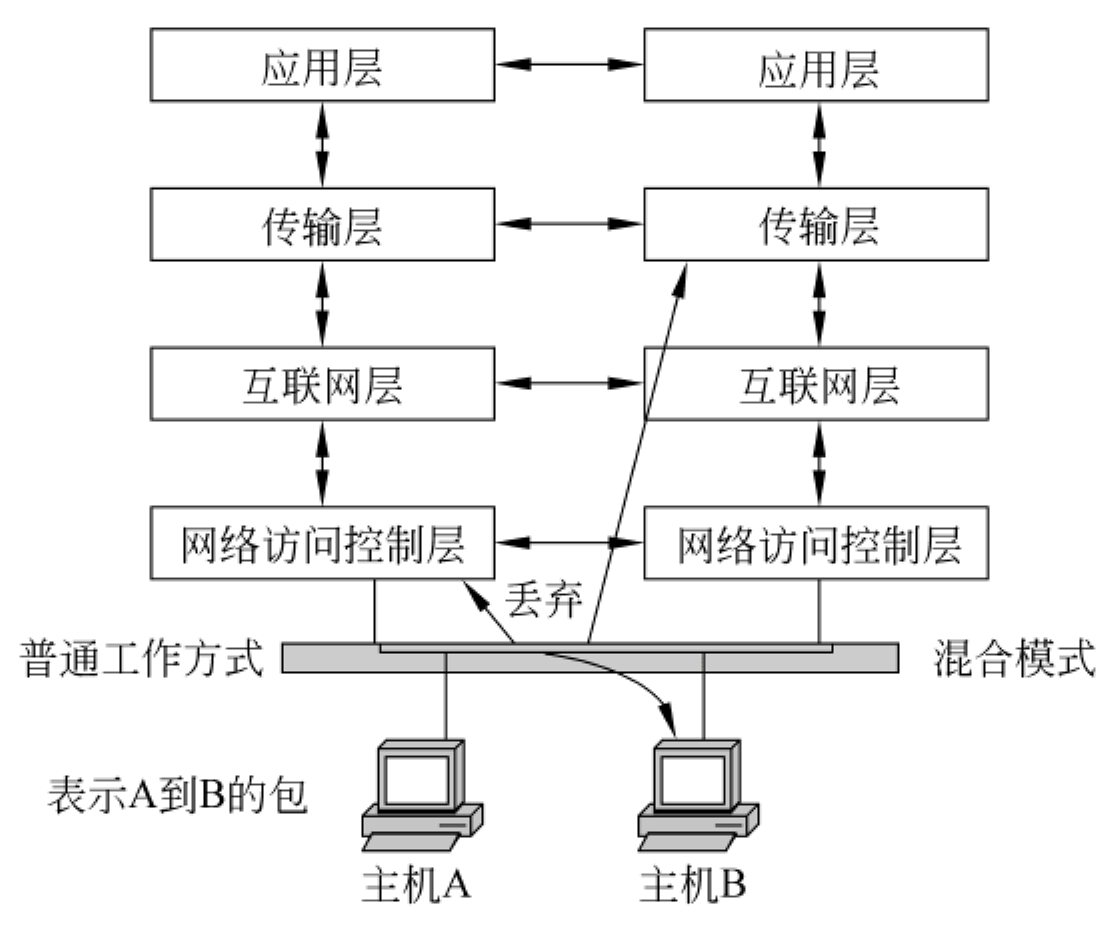


图 2.14 以太网卡混合工作方式和普通工作方式

Internet 上的信息容易被窃听和劫获的另一个原因是，当有一个人用一台主机和网络上的另一台主机进行通信时，它们之间相互发送的数据信息包是经过很多机器(网络和路由器)重新转发的。如在公司计算机局域网上的一台主机上要访问 Hotmail 主机，用户数据包要经过公司局域网的路由器或代理服务器、公司网络的路由器、网络服务商的多个路由器，然后从总出口出国，再经过很多网络和路由器才能到达 Hotmail 主机。具体要经过多少主机、多少路由器和多少网络，不同的时候可能不同，用户可以用网络测试工具得到。图 2.15 表示了网络上数据信息层层传递的工作原理。

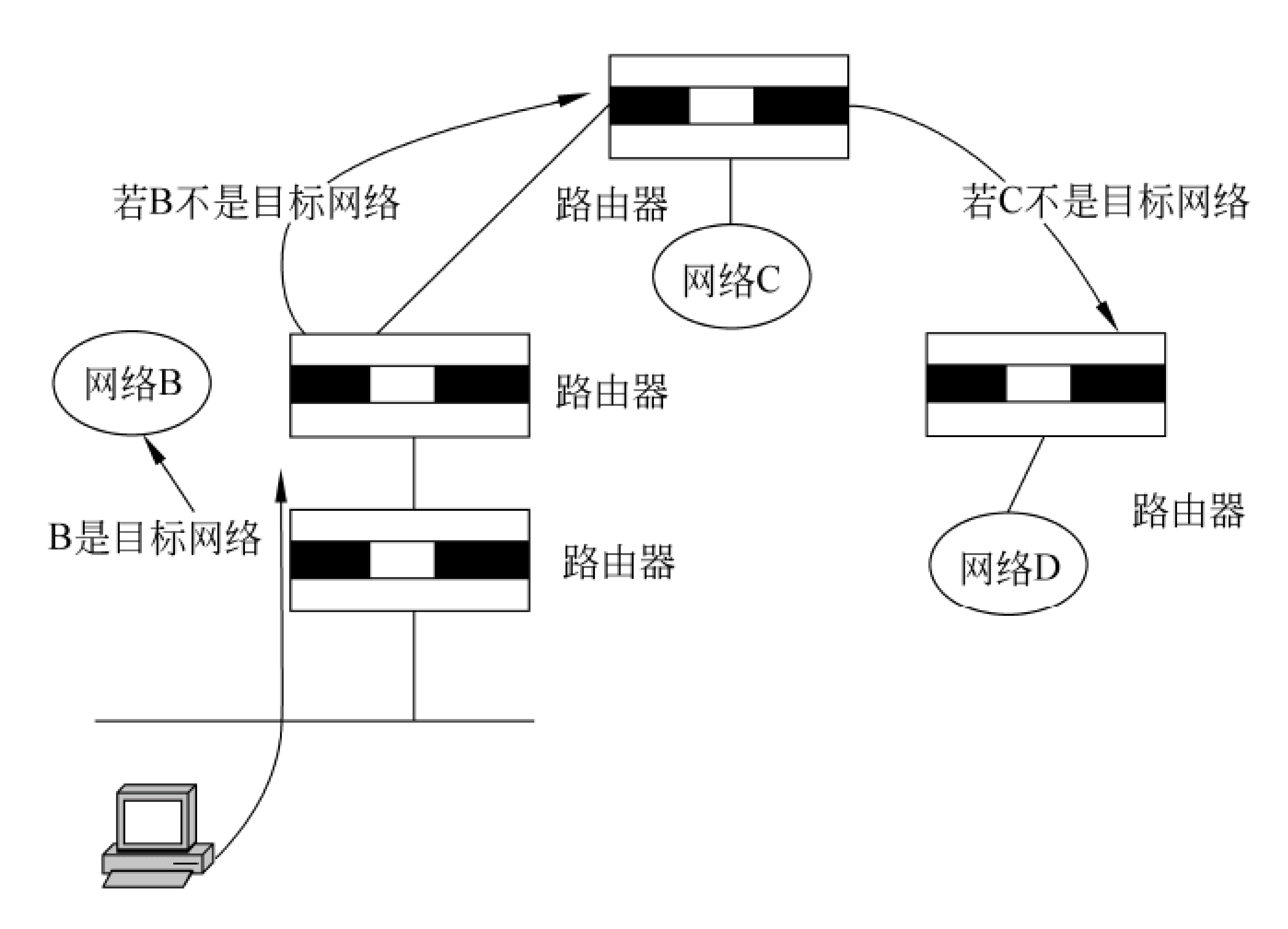


图 2.15 Internet 上数据的传输过程

Internet 的这种工作原理不仅节约了资源，而且简化了传输过程，符合 TCP/IP 协议简单、高效的宗旨，但这也带来了安全上的隐患。当然用户不可能力求安全而放弃这种方法，因为这样做是不实际的，也是没有必要的。用户所能做的只是意识到这种问题，并想办法来解决这种问题，提高系统的安全性。在数据的传输过程中，如果一个黑客可以使用一台处于用户的数据包传输路径上的主机，那么他就可以窃听或劫持用户的数据包。例如，处于每个网络出口上的机器(如网络上的边界路由器)就可以监听所有从这个网络进出的数据包，这和以前经过总机接转的电话监听是类似的。实际上，网络流量的统计和防火墙等都是利用了这个原理来实现的。网络上的窃听可能是出于好奇，也可能是恶意的。现在，越来越多的黑客不再是喜欢破坏公物的人，而多数是出于商业目的，所以网络安全是把 Internet 真正推向商业化所必须要考虑和解决的问题。图 2.16 表示了这种类型的窃听过程。

电子欺骗(spoofing attack)是针对 HTTP、FTP 和 DNS 等协议的攻击，可以窃取普通用户甚至超级用户的权限，任意修改信息内容，造成巨大的危害。常见的电子欺骗有 DNS(domain name service)欺骗和 IP 地址欺骗两种。

电子欺骗的一种形式是 DNS 欺骗，它是利用了 DNS 服务本身的脆弱性。DNS 是其他 Internet 服务，如 WWW 服务、FTP 服务和电子邮件服务 SNMP 的基础，它负责把输入的域名转换成 IP 地址。

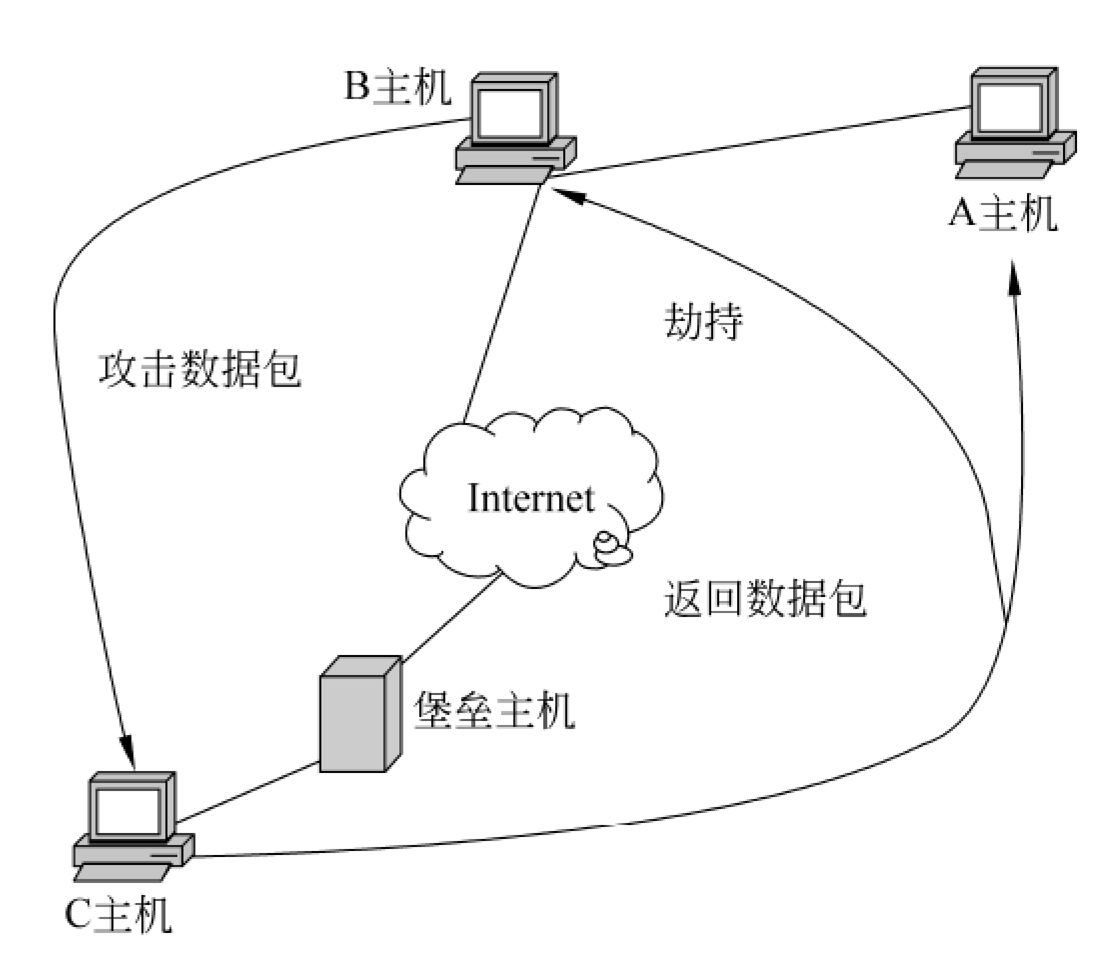


图 2.16 数据在传输过程中被窃听或劫持

网络上的 DNS 服务器很多,这些服务器里有一个数据库,它记录着 IP 地址和域名的对应信息。当用户的主机向这些服务器查询转换信息时,这些主机就会回答用户的查询,从而得到要查找的主机的 IP 地址。DNS 欺骗的关键在于这些服务器不一定知道用户所要的信息,于是该服务器会向别的服务器查询,并且对查询结果不加确认就放入自己的数据库中,还回答用户的查询。在现实生活中有这样的例子,用户想知道 D 是不是一个可信任的人,于是去问 A,可是 A 不能回答这个问题,于是 A 就去问 B,B 知道 D 是不可信任的,于是告诉 A,然后由 A 再告诉用户。试想,D 为了不让用户知道他的真实面目,会设法让他的好友告诉 A 自己是可信任的,而 A 又是一个不负责任的人,他不会去核实这个消息,于是当有用户再次去问 A 时,A 会告诉用户 D 是一个可以信任的人。这就是为什么会有 DNS 欺骗的原因。图 2.17 描述了 DNS 欺骗的过程。

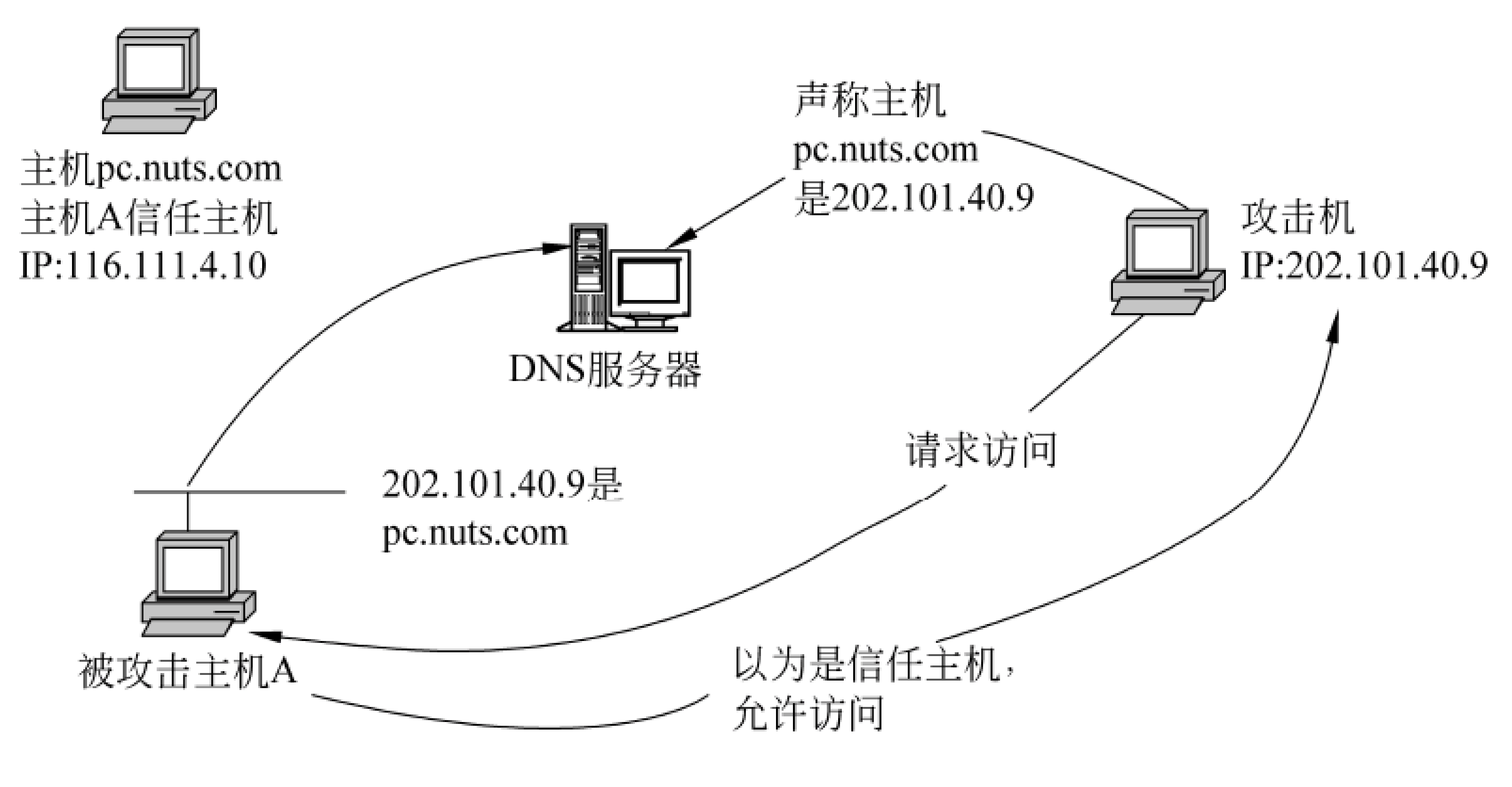


图 2.17 DNS 欺骗

IP 地址欺骗也是一种电子欺骗,也就是伪造他人的源 IP 地址,其实质是让一台机器来扮演另一台机器,借以达到蒙混过关的目的。Internet 上的每一台主机都有一个 IP 地址,当用户的数据包将要离开主机网卡端口时,数据包被自动加上主机的 IP 地址,这样接

收者就知道是谁发来的数据信息。因为 TCP/IP 协议的实现代码是公开的，所以人们能很容易地开发出一种工具软件，让使用者指定数据包的源 IP 地址，实现 IP 地址伪装，从而产生欺骗行为。下面一些服务相对来说容易招致此类攻击。

(1) 任何使用 sunrpc 调用的配置。rpc 指 Sun 公司的远程过程调用标准，是一组工作于网络之上的处理系统调用的方法。

(2) 任何利用 IP 地址认证的网络服务。

(3) X-Window 系统。

(4) 各种 r 服务，在 UNIX 环境中，r 服务包括 rlogin 和 rsh，其中 r 表示远程。人们设计这两个应用程序的初衷是向用户提供远程访问 Internet 网络上主机的服务。r 服务极易受到 IP 欺骗的攻击。

假如黑客主机 C 攻击 A 主机，并且打算伪装成 B 主机和 A 主机进行会话。黑客从 C 主机发出 TCP 连接请求，但使用了 B 主机的 IP 地址，A 主机在收到请求数据包后，向 B 主机发出应答数据包。黑客不会让 B 主机收到 A 主机发出的应答数据包，因为那样 A 主机会知道有人在冒充 B 主机。使 B 主机不能接收到 A 主机发出的应答数据包的方法有三种，第一种是劫持 A 主机发出的数据包；第二种是用大量的连接请求数据包淹没 B 主机，使它无机会处理来自 A 主机的数据包；第三种是改变 A 主机到 B 主机的路由，使数据包不能到达 B 主机，于是黑客就可以在 A 主机不察觉的情况下冒充 B 主机进行对话了。图 2.18 描述了这个过程。

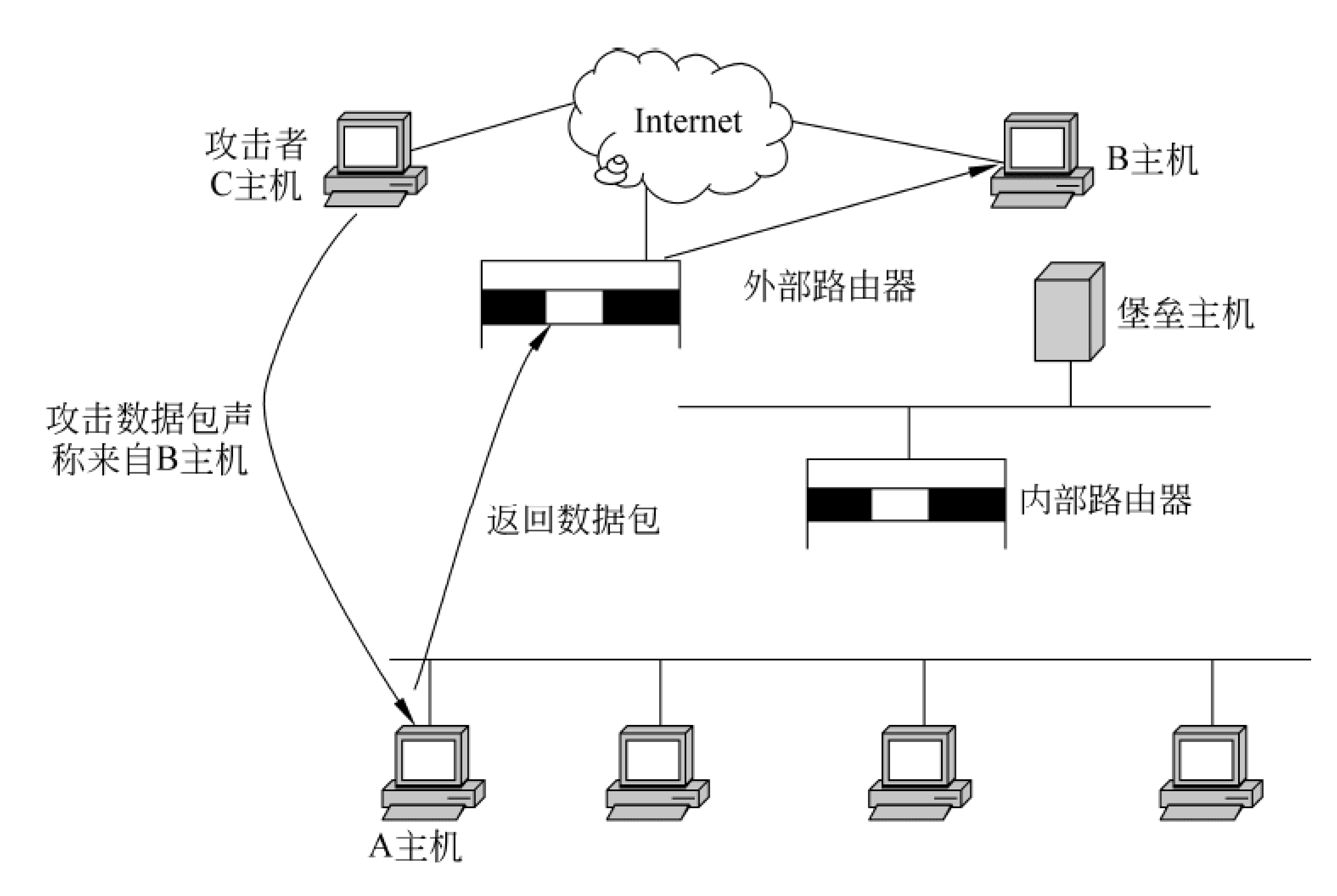


图 2.18 IP 地址欺骗

几乎所有的电子欺骗都依赖于目标网络的信任关系，解决电子欺骗的途径是慎重设置和处理网络中的主机信任关系，尤其是不同网络之间主机的信任关系。如只存在局域网内的信任关系，可以设置路由器使之过滤掉外部网络中自称源地址为内部网络地址的 IP 数据包，来抵御 IP 欺骗。目前，Cisco System 和 ISS 等公司提供的一些安全软件包具有测试网络在 IP 欺骗上的漏洞的功能。

223 脆弱的TCP/IP服务

基于TCP/IP协议的Internet服务很多,有WWW服务、FTP服务和电子邮件服务、TFTP服务、NFS服务和Finger服务等。这些服务都存在不同程度的安全缺陷。当用户用防火墙保护站点时,就应该清楚提供哪些服务、禁止哪些服务。

1. 电子邮件服务

电子邮件服务给人们提供了一种便宜、方便和快捷的服务,电子邮件地址甚至开始出现在人们的名片上了,成了最受欢迎的通信方式之一。现在,UNIX操作系统环境下的电子邮件服务器一般是用Sendmail,它是一个复杂且功能强大的应用软件,正因为如此,它的安全漏洞很多。一般来说,程序越庞大、越复杂,出现安全漏洞的可能性就越大。Sendmail在UNIX操作系统环境下以root账号运行,所以如果该程序被黑客利用,用户主机的损失将十分巨大。Internet上的蠕虫病毒曾经震惊世界,它使大批的网络服务器陷于瘫痪,这种病毒就是利用了Sendmail的安全缺陷。如果使这些功能以更安全的方式实现,则需要对Sendmail进行重新设计和重新实现,但人们又会担心新的版本会出现更多未知的安全漏洞。Sendmail的安全问题被人们修修补补,但总有新的问题出现。

除此之外,电子邮件附件中的文件可能会带有病毒,也给系统安全带来了麻烦。电子邮件炸弹就是一个令人头疼的问题。

2. FTP服务

FTP服务是用于传输文件的,可以用来下载任何类型的文件。网络上有许多匿名FTP服务站点,其上有许多免费软件、图片和游戏等软件,匿名FTP是人们常使用的一种服务方式。匿名FTP服务就像匿名WWW服务一样是不需要口令的,但用户的权利会受到严格的限制。匿名FTP存在一定的安全隐患,因为有些匿名FTP站点提供可写空间给用户,这样黑客可以上传一些软件到站点上浪费用户的磁盘空间、网络带宽等系统资源,还可能会造成“拒绝服务”攻击。匿名FTP服务的安全在很大程度上取决于一个系统管理员的水平,一个低水平的系统管理员很可能会错误授权配置,从而被黑客加以利用,以致破坏整个系统。

3. Finger服务

Finger服务用于查询用户的信息,包括网上成员的真实姓名、用户名、最近的登录时间和地点等,也可以用来显示当前登录在机器上的所有用户名,这对于入侵者来说是无价之宝,因为它能告诉入侵者在本机器上有效的登录名,然后入侵就可以注意其活动了,等待时机成熟时进行入侵,实施攻击。

4. 其他安全性极差的服务

除了上面提到的服务外,还有如WWW、X-Window系统服务,基于RPC的NFS服务和BSD UNIX系统的“r”开头的服务,如rlogin、rsh和rexec等。这些服务的安全性极

差,一般只在内部使用。如果网络有防火墙,就应该把这些服务限制在内部网络中。

2.2.4 来自 Internet 的威胁

Internet 上存在人的威胁和自然的破坏。在这两个因素中,人为的破坏是更重要的,自然的破坏可以通过数据备份和冗余设置等来预防,人为的破坏则是防不胜防的。人为的破坏主要来自网络黑客,研究计算机网络犯罪现在已经成为犯罪学研究领域的一个重要部分,这些罪犯知识水平高、危害性大,而且隐蔽性很强,是一种高科技手段的犯罪行为。目前,在 Internet 上实行商业信息盗窃、银行抢劫等的犯罪活动越来越多,网络黑客不仅是一些想显示自己计算机水平和计算机应用能力的好奇的大学生,更多的是一些专职的商业间谍,有的出于对钱财的贪婪,有的是出于其他目的。还有人为的破坏来自网络内部,这种危害来自那些对企业或单位不满,或者是被解雇了的职员对内部网络的入侵,因为这种人对内部网络很了解,他们的这种入侵危害性很大。因此,网络管理人员及时地删除离职人员的账户是非常重要的。

除了直接的网络入侵外,各种病毒程序也是 Internet 上的潜在威胁,这些病毒可以在网络上随意传播,也可以通过下载的软件,如 Java 程序、ActiveX 控件等进入内部网络,从而对网络造成危害。特洛伊木马就是一种病毒程序,它在表面上看起来是无害的,具有很强的隐蔽性,但它实际上却在背后破坏用户的网络。

虽然现在的防火墙都声称具有防病毒的功能,但新的病毒、旧病毒的变异品种是不会被发现的,它仍然会进入用户的网络,给网络造成危害。

2.3 网络协议存在的不安全性

网络层的协议是一些传输透明化的协议,如果不使用一些监视系统进程的工具,用户是看不见这些协议的。

Sniffers 是一种能看到这些步骤的装置,这个装置可以是软件,也可以是硬件,它能读取通过网络发送的每一个数据包,能读取发生在网络层协议的任何活动。它广泛地用于隔离用户看不到的、网络性能下降的问题,它会对网络的安全问题造成威胁。

网络层协议包括地址解析协议、Internet 控制消息协议、Internet 协议、传输控制协议等。

2.3.1 IP协议与路由

1. IP 协议

IP 协议定义了一种高效、不可靠和无连接的传输方式。由于传输没有得到确认,所以是不可靠的。一个数据包可能丢失了,或看不见了,或延时了,或传输顺序错了,但是传输设备并不检测这些情况,也不通知通信双方。无连接则是因为每个数据包的传递与别的数据包是相互独立的,同一个计算机上的数据包可以通过不同的路径到达另一台计算机,或在别的计算机上已经丢失。由于传输设备都试图以最快的速度传输,所以是最高

效的。

IP 协议定义了通过 TCP/IP 网络传输的数据格式，定义了数据进行传递的路由功能。IP 数据包由一个头和数据部分组成，数据包的头部分包含诸如目的地址、源地址和数据类型等信息。

2. IP 路由

一个网络上连接着两种基本设备——主机和路由器，路由器通常连接几个物理网络。对一台主机来讲，要将一个数据包发送到别的网络，就需要知道这个数据包应该走什么路径才能到达目的地。对一台路由器来讲，必须清楚将收到的数据包发往哪个物理网络。因此，无论主机还是路由器，在发送数据包时都要做路由选择。

数据发送有直接数据发送和间接数据发送两种方式。直接数据发送通常是在同一个物理网络里进行的。当一个主机或路由器要将数据包发送到同一物理网络上的主机时，就是采用这种方式的。先判断 IP 数据包中的目的地址中的网络部分，如果是在同一个网络上，则通过地址分析，将 IP 数据包的目的地址转换成物理地址，并将数据包解开，和该地址合成一个物理传输帧，通过局域网将数据包发出。间接数据发送是在不同物理网络之间进行的。当一个主机或路由器要将数据包发送到不同的物理网络上的主机时，这台设备就先在路由表中查找路由，然后将数据包发往路由中指定的下一个路由器，这样一直向外传送数据包，最后肯定有一个路由器发现数据包要发往同一个物理网络，于是，再用直接数据发送方式将数据包发到目的主机上。

主机和路由器在决定数据怎样发送的时候，都要去查找路由。一般都将路由组成一个路由表存放在计算机中。路由表一般采用(N,R)对表示，N 是目的地址的网络地址，R 是传输路径中的下一个路由。通常这个路由和这台计算机在同一个物理网络里。

2.3.2 TCP 协议

TCP 协议在 IP 协议之上，为其上的应用层提供了一种可靠的传输服务，这种服务的特点是可靠、全双工、流式和无结构传输。

TCP 协议使用一种叫积极确认和重发送技术来实现可靠传输。接收者在收到发送者发送的数据后，必须发一个相应的确认(ACK)消息，表示它已经收到了数据。发送者保存发送的数据的记录，在发送下一个数据之前，等待这个数据的确认消息。在发送这个数据的同时，发送者还启动一个计时器，如果在一定的时间之内，没有接收到确认消息，就认为这个数据在传送时丢失了，接着就会重新发送这个数据。

这种方法产生了一个问题，就是数据包的重复。如果网络传输速度比较低，等到等待时间结束后，确认消息才返回到发送者，那么由于发送者采用的重复发送方法，就会出现重复的数据包了。解决的办法之一是给每个数据包分配一个序列号，并需要发送者记住哪个序列号的数据包已经确认了。为了防止由于延时或重复确认，规定确认消息里也要包含确认序列号，从而发送者就能知道哪个数据包已经确认了。

使用 TCP 传输就是建立一个连接，在 TCP 传输中一个连接由两个端点组成。其实一个连接代表的是发送者和接收者两端应用程序之间的一个通信，可以把它们想象成建

立了一个电路，通常一个连接用(Host，Port)表达，Host 是主机，Port 是端口。TCP 端口能被几个应用程序共享。对于程序员来讲，可以理解为一个程序可以为不同的连接服务。

TCP 传输数据的单位是段，在建立连接、发送数据、确认消息和告知窗口大小时均要进行段的交换。段的格式也分成头和数据两个部分。

TCP 协议使用三次握手来建立一个 TCP 连接。握手过程的第一个段的代码位设置为 SYN，序列号为 x，表示开始第一次握手，接收方收到这个段后，向发送者回发一个段，代码位设置为 SYN 和 ACK，序列号设置为 y，确认序列号设置为 x+1。发送者收到这个段后，就知道可以进行 TCP 数据发送了，于是它又向接收者发送一个 ACK 段，表示双方的连接已经建立。在完成握手之后，就开始正式的数据传输了。

TCP 协议的这种属性决定了它难以避免的安全隐患，目前在 Internet 上的安全问题中，很多攻击方式都是建立在 TCP 欺骗的基础之上的。

2.3.3 Telnet 协议

Telnet 协议的目的就是提供一个相当通用的、双向的、面向 8 位字节的通信机制。它的最初目的是允许在终端和面向终端的进程之间进行的交互。Telnet 不仅允许用户登录到一个远程主机上，还允许用户在那台计算机上执行命令。这样，用户在自己的局域网里的任何一台计算机上就可以 Telnet 到清华大学计算机校园网络上的一台计算机，并在这台计算机上运行程序。Telnet 没有图形功能，它仅提供基于字符界面的访问。

即使 GUI 应用程序被广泛采用，Telnet 这个建立在字符基础上的应用程序仍相当地流行，其原因如下。

(1) Telnet 允许用户以很小的网络资源花费实现各种功能(如收发电子邮件)。

(2) 实现安全的 Telnet 是件十分简单的事，有许多这样的程序，通用的是 Secure Shell。要使用 Telnet，用户必须指定启动 Telnet 客户的命令，并在后面指定目标主机的名字。在 Linux 中，可以这样：$ telnet sctc. edu. cn，这个命令启动 Telnet 过程，连接到 sctc. edu. cn 网络的一个服务器上。这个连接可能被接受，或被拒绝，这与目标主机的配置有关。

Telnet 并不是一种非常安全的服务，虽然登录时它要求用户认证，但由于 Telnet 发送的信息都未加密，所以信息容易被网络监听。仅当远程计算机及其与本地站点之间的网络通信安全时，Telnet 才是安全的。这就意味着在 Internet 上 Telnet 是不安全的。

除了 Telnet，还有几种程序能用于远程终端访问和执行程序，如 rlogin、rsh 和 on。在受托的环境里使用这些程序，允许用户远程登录而无须重新输入口令。他们登录的主机相信用户所用的主机已对其用户做过认证。但是使用这几个 r 命令是特别不安全的，容易受到 IP 欺骗和名字欺骗及其他欺骗技术的攻击，因此，托管主机模式并不适合在 Internet 上使用。

在设有防火墙保护的网络内使用 rlogin 和 rsh 是可以的，这取决于企业内部的安全措施。然而，on 依靠客户机程序进行安全检查，每个人都可以假冒客户机而回避检查。因此，on 是很不安全的，即使在设有防火墙的局域网内使用也是如此，最好使 on 命令失效。



【案例】 Telnet 漏洞攻击与防范

案例分析

Telnet 是 Internet 上远程登录的一种程序;如果拥有登录账号及密码,使用者可以通过网络登录到网络另一端的计算机上,甚至还可以存取那台计算机上的文件。黑客可以利用这个程序远程入侵到目标主机。

操作环境

(1) 局域网主机。

(2) Windows XP/2000/2003 系统。

操作步骤

第 1 步 建立 IPC $ 连接(假设使用 X-scan 扫描器扫描到目标主机账号为 administrator,密码为空),如图 2.19 所示。

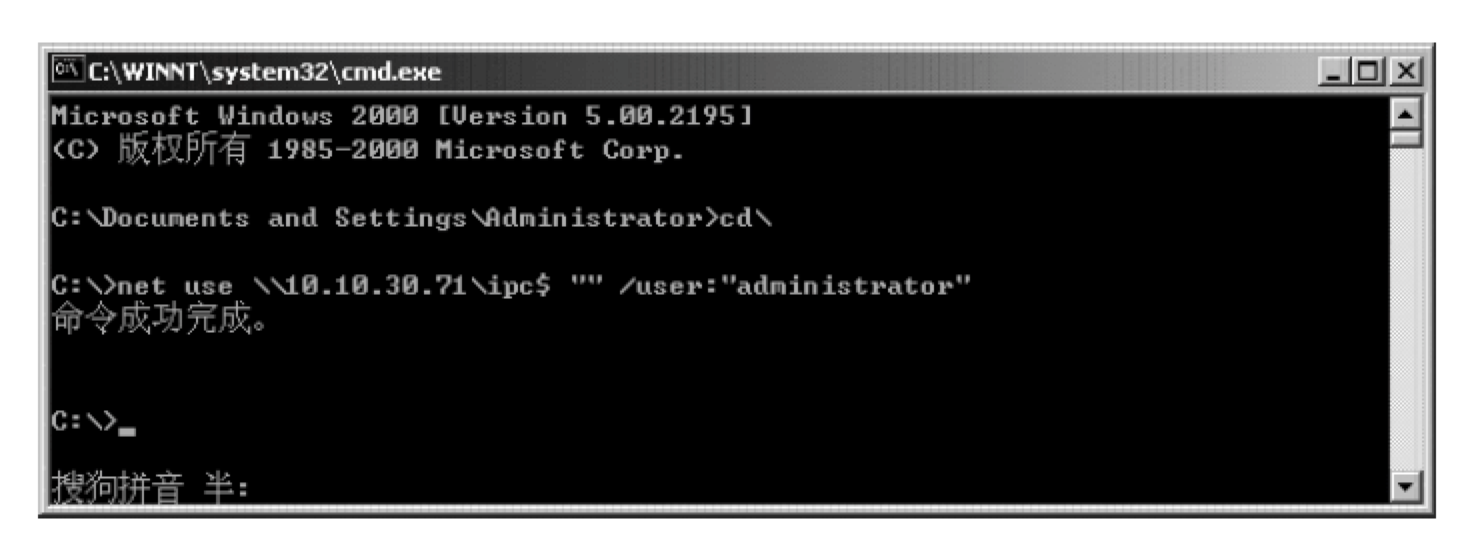


图 2.19 建立 IPC $ 连接

第 2 步 开启远程主机中被禁用的 Telnet 服务,如图 2.20 所示。

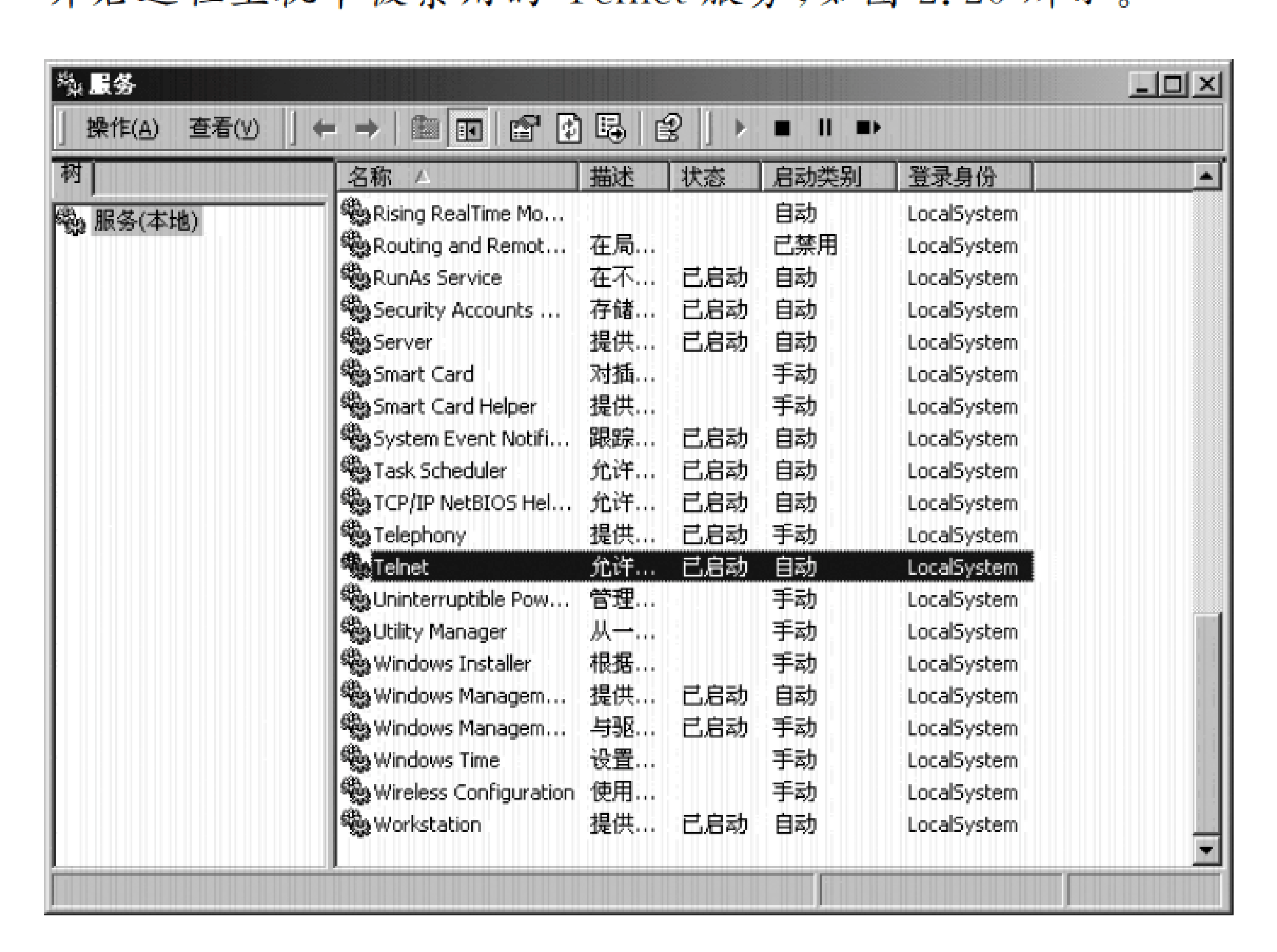


图 2.20 开启远程主机中被禁用的 Telnet 服务

第 3 步　断开 IPC $ 连接，如图 2.21 所示。



图 2.21　断开 IPC $ 连接

第 4 步　在本地计算机上打开 MS-DOS 界面，然后用该 MS-DOS 进行 Telnet 登录，如图 2.22 所示。

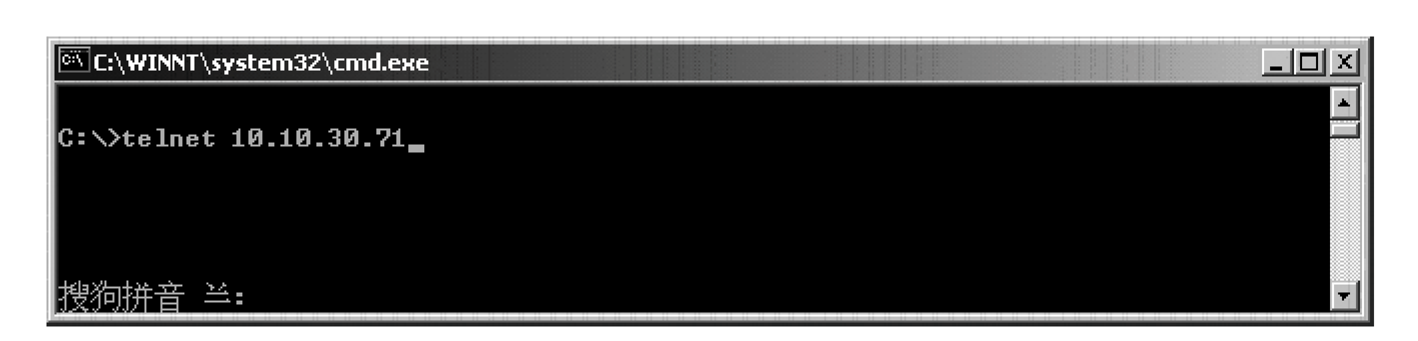


图 2.22　Telnet 登录

第 5 步　输入"telnet 10.10.30.71"命令并按 Enter 键后，在打开的界面中输入 y 表示发送密码并登录，如图 2.23 所示。



图 2.23　输入 y

图 2.24 所示为登录成功后的界面。

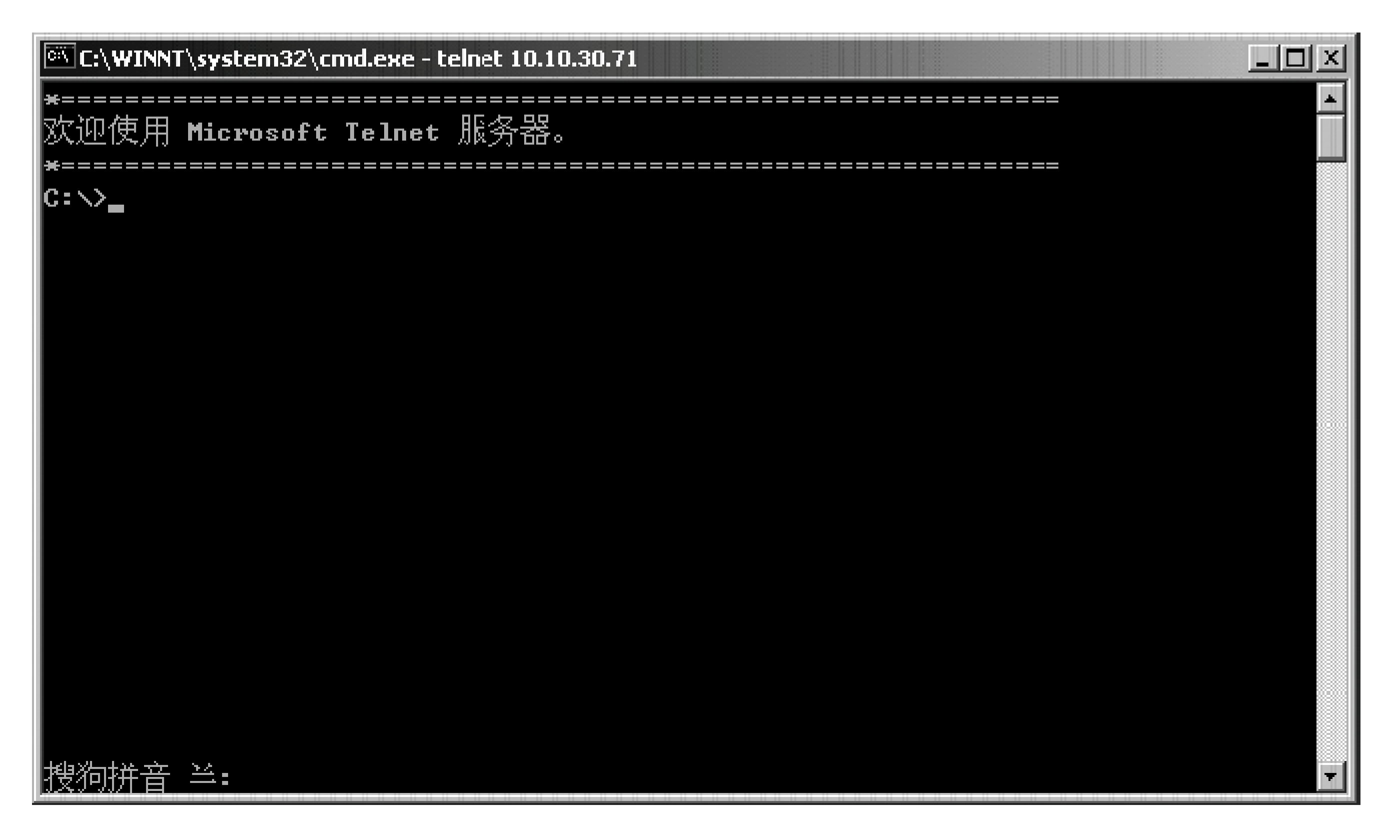


图 2.24　登录成功后的界面

第 6 步 图 2.24 就是远程主机为 Telnet 终端用户打开的 Shell，在该 Shell 中输入的命令将会直接在远程计算机上执行。例如，输入“net user”命令来查看远程主机上的用户列表，如图 2.25 所示。



图 2.25 查看远程主机上的用户列表

2.3.4 文件传输协议

文件传输协议(FTP)是从一个系统向另一个系统传递文件的标准方法，它的目标如下。

(1) 促进文件和程序的共享。

(2) 鼓励间接和含蓄地使用远程计算机。

(3) 使用户不必面对主机间使用的不同的文件存储系统。

(4) 有效和可靠地传输文件。

FTP 应用在 C/S(Client/Server)环境。请求计算机启动一个 FTP 客户端软件，这就给目标文件服务器发出了一个请求。这个要求被送到端口 21。一个连接建立起来后，目标文件服务器必须运行一个 FTP 服务软件。

大多数站点担心的是用户会带入有破坏性的软件及一些计算机游戏、盗版软件和黄色图片，这些东西花费大量的机时并占用磁盘空间，但这并不是主要的安全危险。在进行 FTP 传输时应当注意，千万不要轻信通过 FTP 传来的任何软件。

对于使用匿名 FTP 服务，用户可以用“匿名”用户名登录 FTP 服务器。通常情况下，这要求用户提供完整的电子邮件地址作为响应。然而在大多数站点上，这个要求不是强制性的，只要它看起来像电子邮件地址(如是否包含@符号)，它不对口令做任何方式的校验。要确保匿名 FTP 服务器只能存取允许存取的信息，不允许外人存取本机的其他资料，如私人资料等。在 FTP 服务器处理匿名用户命令之前，许多 FTP 服务器执行 chroot 命令进入匿名 FTP 区。然而为了支持匿名 FTP 和用户 FTP，FTP 服务器要访问所有的文件，这就是说 FTP 服务器并总是在 chroot 环境中运行。

为了解决这个问题，可以通过修改系统的配置来代替直接启动 FTP 服务器，它执行 chroot，然后再启动 FTP 服务器。建立匿名 FTP 系统的具体技术依赖于操作系统使用的特定 FTP 管理程序(守护程序)。

匿名用户获取到的不应见到的文件，通常是由于内部客户将文件放在匿名 FTP 区而实现的。如果不希望外界阅读自己的文件，最好不要给匿名的 FTP 提供文件。匿名

FTP 区的可写路径无论使用何种 FTP 守护程序，都将面临一个特殊的问题：匿名 FTP 区的可写性。站点经常为此区提供空间，以便外部用户能用它上传文件。

可写区是非常重要的，但也有不安全的因素。因为这样的可写路径一旦被发现，就会被 Internet 上的“地下用户”用做“仓库”和非法资料的集散地。

本 章 小 结

计算机网络的基础是网络通信协议，保证通信协议的安全对计算机网络的安全有重要的意义。

TCP/IP 协议本身在设计上就是不安全的，主要存在以下的安全缺陷：网络容易被窃听和欺骗；TCP/IP 服务具有脆弱性；缺乏安全策略；受到来自 Internet 上的威胁。

本 章 练 习

一、填空题

1. TCP/IP 协议族中最重要的两个核心协议是________协议与________协议。
2. 说 TCP/IP 协议本身在设计上就是不安全的，主要存在________、________、________、________的安全缺陷。
3. 电子欺骗是针对________等协议的攻击。
4. IP 欺骗，就是伪造他人的________。
5. 基于 TCP/IP 协议的 Internet 服务有________、________、________、________、________等。

二、简答题

1. 什么是 TCP/IP 协议？试述它的工作原理。
2. TCP/IP 协议存在哪些安全问题？
3. 网络本身存在哪些安全问题？
4. 网络为什么是不安全的？
5. Internet 上存在哪些威胁？
6. 什么是电子欺骗？电子欺骗有哪些形式？
7. FTP 存在哪些安全隐患？如何解决？

实训 数据包的捕获分析

实训目的

通过实训理解网络嗅探的原理，掌握捕获数据包的方法。

实训环境

Windows 操作系统，Sniffer Portable 软件，局域网。

实训步骤

第 1 步 建立网络数据包嗅探环境。

(1) 硬件连接。以 3 台计算机为一组，分别命名为 text1、text2 和 text3，通过交换机连接到一起，两台计算机之间进行正常通信，第三台计算机对其进行数据包捕获操作。

(2) 网络配置。配置 3 台计算机的 IP 地址为同一网段内的不同 IP 地址。

第 2 步 捕获并分析数据。

(1) 计算机 text1 使用 Ping 命令向计算机 text2 发送 ICMP 包，使用计算机 text3 进行捕获，观察捕获数据包，说明使用 Ping 命令建立连接和返回应答的过程，并查看数据包的内容。

(2) 计算机 text2 开启 IIS，建立 WWW 和 FTP 服务。使用计算机 text1 访问计算机 text2 的 WWW 网页和通过 FTP 进行上传与下载。计算机 text3 捕获 text1 与 text2 之间的数据包，分析建立连接的过程及观察捕获的数据包内容。

(3) 观察能否捕获 FTP 登录时的账户名和密码。

第 3 步 有针对性地捕获。

设置捕获策略，仅捕获计算机 text1 从计算机 text2 获取的网页内容。

第 3 章 数据加密技术

Chapter 3

知识目标

- 了解威胁数据安全的各种因素。
- 掌握传统和现代的数据加密技术及其基本概念。
- 数字签名的概念、原理及应用。

技能目标

- 能够使用对称加密软件加、解密数据。
- 能够使用加密软件 PGP 加、解密数据。
- 能够应用数字签名技术。

密码学是一门古老而深奥的学科,有着悠久、灿烂的历史。最早的密码形式可以追溯到 4000 多年前古埃及人在墓志铭中使用过的类似于象形文字的奇妙符号。从古至今,密码技术一直在社会各个领域,尤其是军事、外交等领域广泛使用。在今天,随着计算机网络和通信技术的发展,密码技术更是得到了前所未有的重视,并迅速普及和发展起来。它已经成为计算机安全研究的一个主要方向。

3.1 密码技术简介

密码学包括两部分内容:编码学和编码分析学。编码学是通过编码技术将被保护信息的形式改变,使编码后的信息除了指定的接收者外其他人无法理解的一门学问,也就是加密算法的研究和设计。编码分析学是研究如何攻破一个密码系统,将被加密的信息恢复,也就是密码破译技术。这两部分内容是矛与盾的关系。密码系统包括 5 个要素:明文信息空间、密文信息空间、密钥空间、加密变换 E 和解密变换 D。图 3.1 给出了密码系统示意图。

- 明文,指加密前的原始信息。
- 密文,指通过加密手段加密后的信息。
- 加密过程,指将明文进行数据转换变成密文的过程。
- 解密过程,指利用加密的逆转换将密文恢复成明文的过程。
- 密钥,指控制加密和解密运算的符号序列。

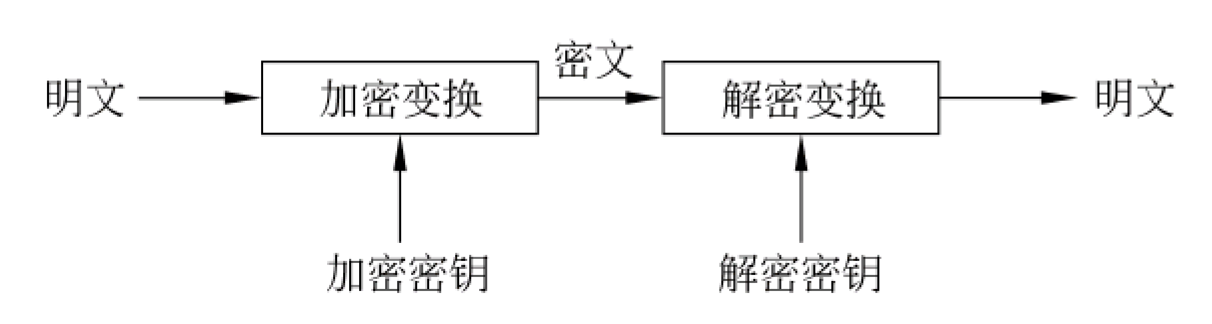


图 3.1 密码系统示意图

密码系统理论上要求使用方便,并且对系统的保密不依赖于对加密算法和解密算法的保密,而只依赖于对密钥的保密。这样,即使密文和对应的明文被截获后,仍不容易进行解密变换。

一个较为成熟的密码体系,其算法应该是公开的,而密钥是保密的。这样,使用者只需简单地修改密钥,就可以达到改变加密过程和加密结果的目的。密钥通常由一小串字符组成,可以选择多种可能的加密过程和加密结果对它进行设计,并且可以按需频繁更换。在加密系统的设计中,密钥的长度是一个主要的设计问题。一个 2 位数字的密钥意味着有 100 种可能性,一个 3 位数字的密钥意味着有 1000 种可能性,一个 6 位数字的密钥意味着有 100 万种可能性。密钥越长,加密系统被破译的几率就越低。

根据数据加密的方式,加密算法可以分为对称密钥加密算法(简称对称算法)和非对称密钥加密算法(简称非对称算法)两种,也称为对称加密技术和非对称加密技术。对称算法是指加密和解密的过程使用同一个密钥。它的特点是运算速度非常快,适用于对数据本身的加/解密操作。常见的对称算法有 DES、TDEA(3DES)、IDEA、AES、MD5 算法等。相对于对称算法来讲,非对称算法的运算速度要慢得多,但是在多人协作或需要身份认证的数据安全应用中,非对称算法的运算具有不可替代的作用。使用非对称算法对数据进行签名,可以证明数据发行者的身份并保证数据在传输的过程中不被篡改。在这种加密算法中有两个密钥,一个称为公钥,一个称为私钥。在加密时,公钥用于加密,私钥用于解密。这种算法比较复杂,如 RSA 算法、PGP 算法等,通常用于数据加密。由于非对称算法的速度较慢,现在多采用对称算法与非对称算法相结合的加密方法,这样,既可以有很高的加密强度,也可以有较快的加密速度。此方法已广泛用于 Internet 的数据加密传送和数字签名。通过对传输的数据进行加密来保障其安全性,已经成为了一项计算机网络系统安全的基本技术,它可以用很小的代价为数据信息提供相当大的安全保护,是一种主动的安全防御策略。

3.2 传统的加密方法

3.2.1 替代密码

在替代密码中,用一组密文字母来代替一组明文字母以隐藏明文,但保持明文字母的位置不变。

最古老的替代密码是恺撒密码,它用 D 表示 a,用 E 表示 b,用 F 表示 c,……,用 C 表示 z,也就是说密文字母相对明文字母左移了 3 位。为清楚起见,一律用小写表示明文,

用大写表示密文，这样明文的“cipher”就变成了密文的“FLSKHU”。以此类推，可以让密文字母相对明文字母左移 k 位，这样 k 就成了加密和解密的密钥。这种密码是很容易被破译的，因为最多只需尝试 25 次（$k=1\sim25$）即可轻松破译密码。

较复杂的密码是明文字母和密文字母之间的映射关系，它没有规律可循，比如将 26 个英文字母随意映射到其他字母上，这种方法称为单字母表替换，其密钥是对应于可能的密钥，即使计算机每微秒试一个密钥，也需要 1013 年。但事实上完全不需要这么做，破译者只要拥有很少一点密文，利用自然语言的逻辑特征，很容易就可破译密码。破译的关键在于找各种字母或字母组合出现的频率，比如经统计发现，英文中字母 e 出现的频率最高，其次是 t、o、a、n、i 等，最常见的两字母组合依次为 th、in、er、re 和 an，最常见的三字母组合依次为 the、ing、and 和 ion。因此，破译者首先可将密文中出现频率最高的字母定为 e，频率次高的字母定为 t……然后猜测最常见的两字母组、三字母组，比如密文中经常出现 tXe，就可以推测 X 很可能就是 h，如经常出现 thYt，则 Y 很可能就是 a 等。采用这种合理的推测，破译者就可以逐句组织出一个试验性的明文。

为了去除密文中字母出现的频率特征，可以使用多张密码字母表，对明文中不同位置上的字母用不同的密码字母表来加密。比如任意选择 26 张不同的单字母密码表，相互间排定一个顺序，然后选择一个简短易记的单词或短语作为密钥，在加密一条明文时，将密钥重复写在明文的上面，则每个明文字母上的密钥字母即指出该明文字母用哪一张单字母密码表来加密。

例如，要加密明文“please execute the latest scheme”，密钥为 computer，则将 computer 重复写在报文上面，如图 3.2 所示。

c	o	m	p	u	t	e	r	c	o	m	p	u	t	…	e	r	c	o	m	p
p	l	e	a	s	e	e	x	e	c	u	t	e	t	…	s	c	h	e	m	e

图 3.2　把一段明文用密钥 computer 进行加密

于是第 1 个明文字母 p 用第 3 张（假设 a～z 分别表示顺序 1～26）单字母密码表加密，第 2 个明文字母 l 用第 12 张单字母密码表加密……显然，同一个明文字母因位置不同而在密文中可能用不同的字母来表示，从而消除了各种字母出现的频率特征。

虽然破译多字母密码表要困难一些，但如果破译者手头有较多的密文，仍然是可以破译的，破译的诀窍在于猜测密钥的长度。首先破译者假设密钥的长度，然后将密文按每行 k 个字母排成若干行，如果猜测正确，那么同一列的密文字母应是用同一单字母密码加密的，因此，同一列中各密文字母的频率分布应与英文相同，即最常用字母（对应明文字母 e）的频率为 13%，次常用字母（对应明文字母 t）的频率为 9%等。如果猜测不正确，则换一个 k 值进行重试，一旦猜测正确，即可逐列用破译单字母表密码的方法进行破译。进一步提高破译难度可以使用比明文更长的密钥，使上述破译方法失效，但这样的密钥难以记忆，必须记在纸上，这就增加了失密的可能性。

3.2.2　换位密码

换位有时也称为排列，它不对明文字母进行变换，只是将明文字母的次序进行重新排

列。图 3.2 是一种常用的换位密码，它的密钥必须是一个不含重复字母的单词或短语，加密时将明文按密钥长度截成若干行排在密钥下面，按照密钥字母在英文字母表中的先后顺序给各列编号，然后按照编好的序号按列输出明文即成密文。换位的步骤如下。

(1) 判断密码类型，检查密文中 E、T、O、A、N、I 等字母出现的频率，如果符合自然语言特征，则说明密文是用换位密码做的。

(2) 猜测密钥的长度，也即列数。在许多情况下，破译者根据消息的上下文，常常可以猜测出消息中可能包含的单词或短语，选择的单词或短语最好长一些，使其至少可能跨越两行，如 latestscheme。将选择的单词或短语按照假定的长度 k 截成几行，由于同一列上相邻的字母在密文中必是相邻的，因此，可以将各列上的各种字母组合记下来，在密文中搜索。如将 latestscheme 按照假设的长度 8 截成两行，则相邻的字母组合有 lh、ae、tm 和 ee。假如设想的 k 是正确的，则大部分设想的字母组合在密文中都会出现；如果搜索不到，则换一个 k 再试。通过寻找各种可能性，破译者常常能够确定密钥的长度。

(3) 确定各列的顺序。如果列数比较少的话，可以逐个检查 $k(k-1)$ 个列对，查看它们的二字母组的频率是否符合英文统计特征，与特征符合最好的列对认为其位置正确。然后从剩下的列中寻找这两列的后继列，如果某列和这两列对组合后，二字母组和三字母组的频率都很好地符合英文统计特征，那么该列就是正确的后继列。通过同构法也可以找到它们的前趋列，直至最终将所有的列序全部找到。图 3.3 是一个换位密码的例子。

C	O	M	P	U	T	E	R	
1	4	3	5	8	7	2	6	明文 pleaseexecutethelatestscheme
p	l	e	a	s	e	e	x	
e	c	u	t	e	t	h	e	密文 PELHEHSCEUTMLCAE ATEEXECDETTBSESA
l	a	t	e	s	t	s	e	
h	e	m	e	a	b	c	d	

图 3.3　一个换位密码的例子

3.3　常用的加密技术

3.3.1　DES 算法

数据加密标准(data encryption standard，DES)是由 IBM 公司研制的加密算法，于 1977 年被美国政府采用，作为商业和非保密信息的加密标准被广泛采用。尽管该算法较复杂，但易于实现。它只对小的分组进行简单的逻辑运算，用硬件和软件实现起来都比较容易，尤其是用硬件实现使该算法的速度加快。

1. DES 算法的描述

DES 算法将信息分成 64bit 的分组，并使用 56bit 长度的密钥。它对每一个分组使用

一种复杂的变位组合、替换，再进行异或运算和其他一些过程，最后生成64bit的加密数据。对每一个分组进行19步处理，每一步的输出是下一步的输入。图3.4显示了DES算法的主要步骤。

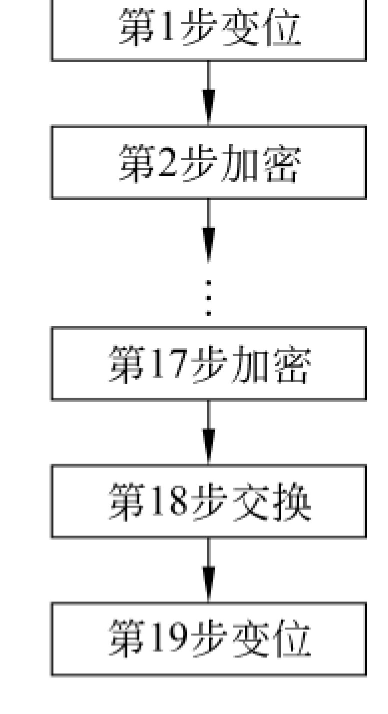


图3.4　DES算法的主要步骤

第一步对64bit数据和56bit密钥进行变位；第2～17步（共16步）除了使用源于原密钥的不同密钥外，每一步的运算过程都相同，包括很多操作；第18步将前32bit与后32bit交换；最后一步是第一步的逆过程，进行另一个变位。

图3.5显示了第2～17步的每一步的主要操作，图中的符号说明如下。

（1）C64，指64bit的待加密信息。

（2）K56，指56bit的密钥。

（3）L32，指C64的前32bit。

（4）R32，指C64的后32bit。

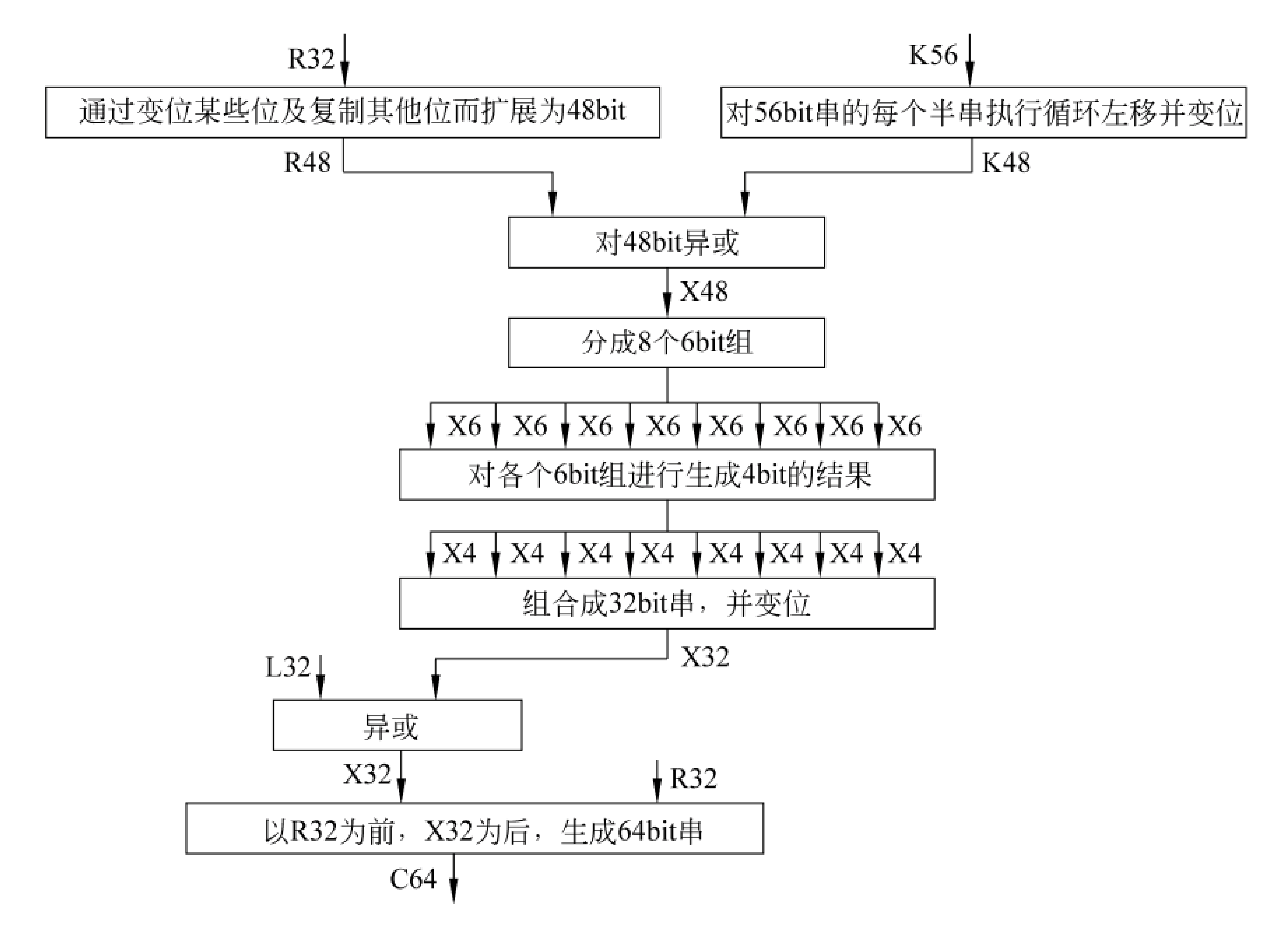


图3.5　DES算法的加密操作流程

其他带下标的字母中的下标都表示bit数，如X48代表处理过程中的48bit的中间bit串。

在每一步中，密钥先移位，再从56bit的密钥中选出48bit。数据后32bit扩展为48bit，并与经过移位和置换的48bit密钥进行一次异或操作，其结果通过8组（每组6bit）输出，将这64bit替代新的32bit数据，再将其变位一次，生成32bit串X32。X32与前半部分的32bit进行异或运算，其结果即成为新的后半部分的32bit，原来的后半部分的32bit成了新的前半部分。将该操作重复16次，就实现了DES的16轮加密运算。

经过精心设计，DES的解密和加密可使用相同的密钥和相同的算法，二者唯一的不同之处是密钥的次序相反。

2. DES算法的安全性

DES算法的加密和解密密钥相同，属于一种对称加密技术。对称加密技术从本质上说都是使用替代密码和换位密码进行加密的。

DES算法的安全性长期以来一直都受到人们的怀疑。主要是因为DES算法的安全性对于密钥的依赖性太强，一旦密钥泄露出去，则跟密文相对应的明文内容就会暴露无遗。DES对密钥的过分依赖使穷举破解成为可能。在早期(20世纪七八十年代)由于专门用于穷举破译DES的并行计算机的造价太高，而且要从256～7112种密钥中找出一种来，还是相当费时、费力的，用DES算法来保护数据是安全的。现在，由于计算机的运算速度、存储容量及跟计算相关的算法都有了比较大的改进，56bit长的密钥对于保密价值高的数据来说已经不够安全了。当然，可以通过增加密钥长度来增加破译的难度进而增强其安全性。

3. 密钥的分发与保护

DES算法加密和解密使用相同的密钥，通信双方进行通信前必须事先约定一个密钥，这种约定密钥的过程称为密钥的分发或交换。关键是如何进行密钥的分发才能在分发的过程中对密钥保密，如果在分发过程中密钥被窃取，再长的密钥也无济于事。

最常用的一种交换密钥的方法是“难题”的使用。“难题”是一个包含潜在密钥的内容，必须去破解。使用难题交换密钥的基本过程如下。

(1) 发送方发送 n 个难题，各用不同的密钥加密。接收方并不知道解密密钥，必须去破解。

(2) 接收方随机选择一个难题并破解它。因为有插入在难题中的模式，使接收方能判断出是否破解。

(3) 接收方从难题中抽出加密密钥，并返回给发送方一个信息指明他破解难题的标识号。

(4) 发送方接收到接收方的返回信息后，双方即按照此难题的密钥进行加密了。

人们可能会问，其他人也可能截获这些难题，他们也可以去破解。关键是他们不知道接收方选择的难题的标识号，即便是他们又截获了接收方返回给发送方的信息，得到难题的标识号，但等他们破解以后，通信双方的通信过程可能已经结束了。

4. 三重数据加密算法

三重数据加密算法(three data encryption algorithm，TDEA)在1985年第一次为金融应用进行了标准化，在1999年合并到数据加密标准中。

TDEA使用3个密钥，按照加密→解密→加密的次序执行3次DES算法。加密、解密的过程如图3.6所示。

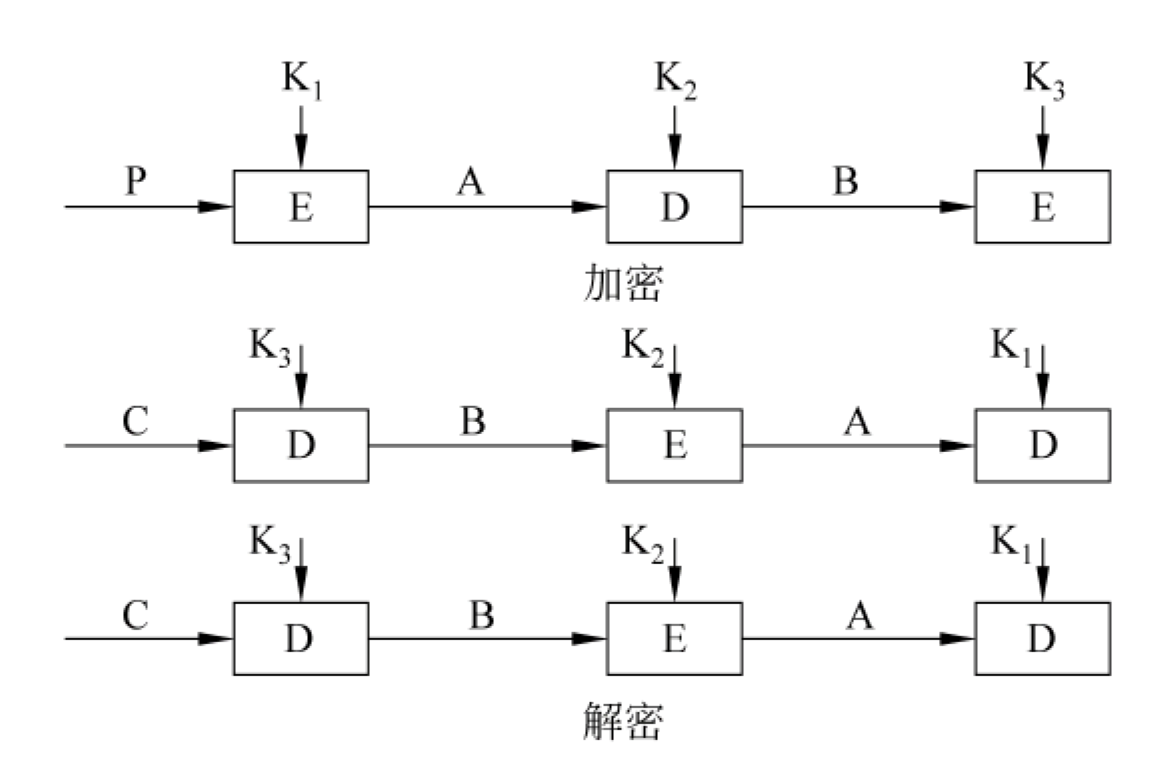


图 3.6　TDEA 的加密、解密过程

图 3.6 中,P 为明文,C 为密文,E 为使用密钥 K_n 加密,D 为使用密钥 K_n 解密。

TDEA 使用 3 个不同的密钥,总有效长度为 168bit,加强了算法的安全性。

5. IDEA 算法

IDEA(国际数据加密算法)是瑞士著名学者提出的。IDEA 是在 DES 算法的基础上发展起来的一种安全、高效的分组密码系统。

IDEA 密码系统的明文和密文长度均为 64bit,密钥长度则为 128bit。其加密由 8 轮类似的运算和输出变换组成,主要有异或、模加和模乘 3 种运算。

IDEA 密码系统在加密和解密运算中,仅仅使用作用于 16bit 子块对的一些基本运算,因此效率很高。IDEA 密码系统具有规则的模块化结构,有利于加快其硬件实现速度。由于 IDEA 的加密和解密过程是相似的,所以有可能采用同一种硬件器件来实现加密和解密。

IDEA 算法的密钥长度为 128bit,是 DES 密钥长度的两倍。它能够抵抗差分密码分析方法和相关密钥分析方法的攻击。科学家已证明 IDEA 算法在其 8 轮迭代的第 4 轮之后便不受差分密码分析的影响了。假定穷举法攻击有效的话,那么即使设计一种每秒钟可以试验 10 亿个密钥的专用芯片,并将 10 亿片这样的芯片用于此项工作,仍需 1013 年才能解决问题。目前,尚无一篇公开发表的试图对 IDEA 进行密码分析的文章。因此,应当说目前 IDEA 是一种安全性好、效率高的分组密码算法。



【案例】 DES 加密技术的应用

案例分析

Apocalypso 软件是一款应用广泛、基于 DES 算法的加密软件。

操作环境

Windows XP/2000/2003 操作系统,Apocalypso 加密软件。

操作步骤

第 1 步 在桌面上创建一个文本文件，取名为 text.txt，如图 3.7 所示。



图 3.7 创建一个文本文件

第 2 步 打开 Apocalypso 软件主界面，准备对文件进行加密，如图 3.8 所示。

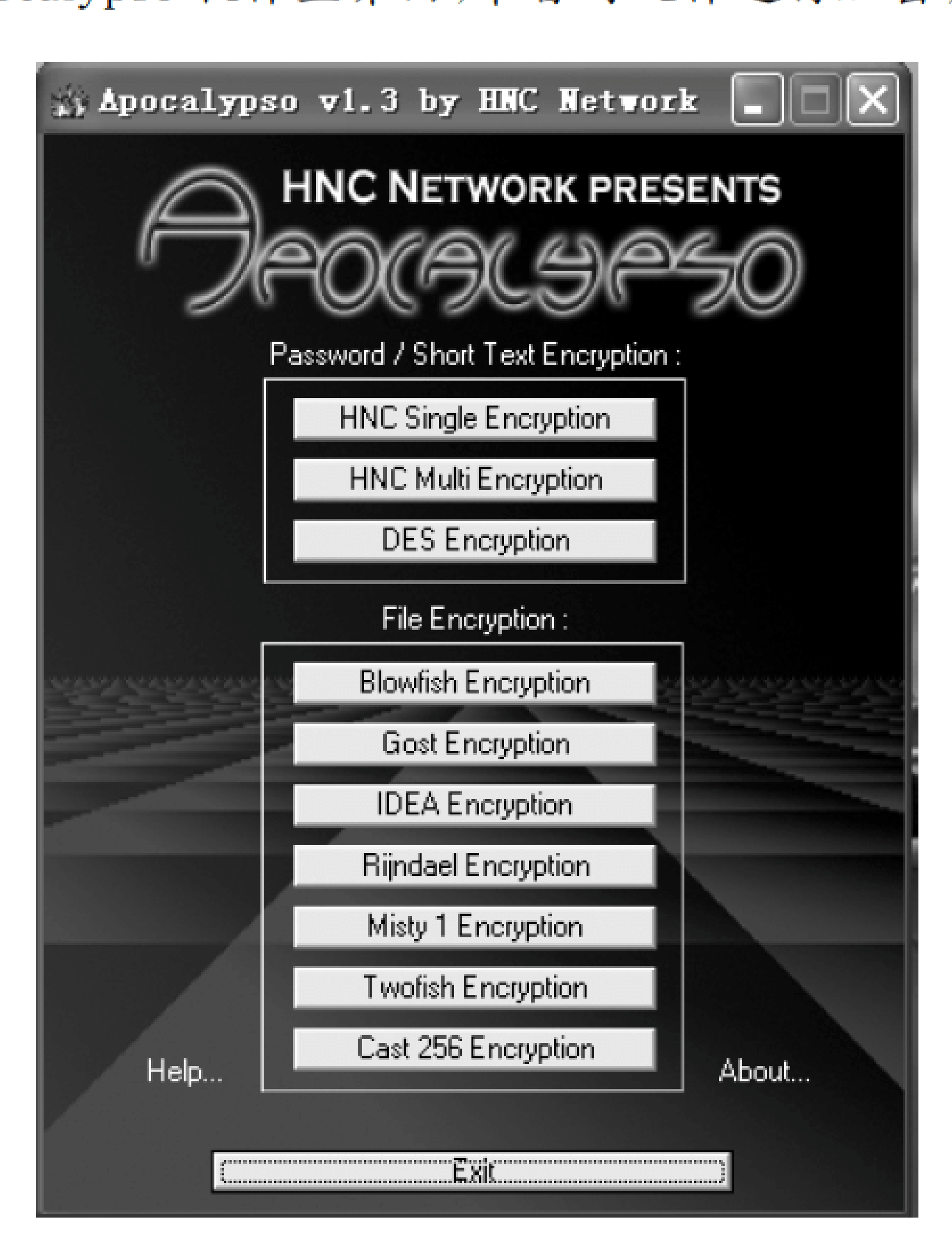


图 3.8 Apocalypso 软件主界面

第 3 步 单击 Blowfish Encryption 按钮，进入文件加、解密界面，如图 3.9 所示。

第 4 步 在 File to be Encrypted/Decrypted 文本框中选择要加密的文件 text.txt，如图 3.10 所示。

第 5 步 在 Output File 文本框中选择加密后文件存放的位置，并将加密后生成的文件取名为 text2.txt，如图 3.11 所示。



图 3.9 文件加、解密界面



图 3.10 选择要加密的文件 text.txt

第 6 步 在 Enter Passphrase here 文本框中输入加密/解密的密码 aa，如图 3.12 所示，然后单击 Encrypt File 按钮，文件开始加密，直到出现加密结束提示，如图 3.13 所示。



图 3.11 选择加密后文件存放的位置



图 3.12 输入加密/解密的密码

第 7 步 找到并打开加密文件 text2.txt，可看到文档内容为乱码，说明已被加密，如图 3.14 所示。



图 3.13 加密结束提示



图 3.14 文档内容

第 8 步 解密。单击 Blowfish Encryption 按钮,进入文件加密/解密界面,在 File to be Encrypted/Decrypted 文本框中选择要解密的文件 text2. txt,在 Output File 文本框中选择解密后文件存放的位置,并将加密后生成的文件取名为 text3. txt,在 Enter Passphrase here 文本框中输入加密/解密的密码 aa,然后单击 Decrypt File 按钮,文件开始解密,如图 3.15 所示,直到出现解密结束提示,如图 3.16 所示。



图 3.15 输入加密/解密的密码 aa



图 3.16 解密结束提示

第 9 步 找到并打开解密后的文件 text3. txt,原密文已恢复为明文,说明文件已被解密,如图 3.17 所示。



图 3.17 文件解密后的内容

3.3.2 RSA 算法

公开密钥加密算法(RSA 算法)展现了密码应用中的一种崭新的思想。它采用非对称加密算法,即加密密钥和解密密钥不同。因此,在采用加密技术进行通信的过程中,不仅加密算法本身可以公开,甚至加密用的密钥也可以公开(为此加密密钥也被称为公钥),而解密密钥由接收方自己保管(为此解密密钥也被称为私钥),增加了保密性。

RSA 算法是由 R. Rivest、A. Shamir 和 L. Adleman 于 1997 年提出的。RSA 的取名就来自于这三位发明者姓的第一个字母。后来,他们在 1982 年创办了以 RSA 命名的公

司 RSA Data Sectrity Inc. 和 RSA 实验室，该公司和实验室在公开密钥密码系统的研究和商业应用推广方面具有举足轻重的地位。

目前，RSA 被广泛应用于各种安全和认证领域，如 Web 服务器和浏览器信息安全、电子邮件的安全和认证、对远程登录的安全保证和各种电子信用卡系统。

RSA 算法使用模运算和大数分解，算法的部分理论基于数学中的数论。下面通过具体实例说明该算法是如何工作的。为了简化起见，在该实例中仅考虑包含大写字母的信息。实际上该算法可以推广到更大的字符集。

1. RSA 算法的加密过程

RSA 算法的加密过程如下。

(1) 为字母制定一个简单的编码，如 A～Z 分别对应 1～26。

(2) 选择一个足够大的数 n，使 n 为两个大的素数(只能被 1 和自身整除的数) p 和 q 的乘积。为便于说明，在此使用 $n=p\times q=3\times 11=33$。

(3) 找出一个数 k，k 与 $(p-1)\times(q-1)$ 互为素数。此例中选择 $k=3$，与 $2\times 10=20$ 互为素数。数字 k 就是加密密钥。根据数论中的理论，这样的数一定存在。

(4) 将要发送的信息分成多个部分，一般可以将多个字母分为一部分。在此例中将每一个字母作为一部分。若信息是 SUZAN，则分为 S、U、Z、A 和 N。

(5) 对每部分，将所有字母的二进制编码串接起来，并转换成整数。在此例中各部分的整数分别为 19、21、26、1 和 14。

(6) 将每个部分扩大到它的 k 次方，并使用模 n 运算，得到密文。在此例中分别是 193 mod 33＝28，213 mod 33＝21，263 mod 33＝20，13 mod 33＝1 和 143 mod 33＝5。接收方收到的加密信息是 28、21、20、1 和 5。

2. RSA 算法的解密过程

(1) 找出一个数 k' 使得 $k\times k'-1=0 \bmod ((p-1)\times(q-1))$，即 $k\times k'-1$ 能被 $(p-1)\times(q-1)$ 整除。k' 的值就是解密密钥。在此例中选择 $k'=7$，$3\times 7-1=20$，$(p-1)\times(q-1)=20$，能被整除。

(2) 将每个密文扩大到它的 k' 次方，并使用模 n 运算，可得到明文。在此例中分别为 287 mod 33＝19，217 mod 33＝21，207 mod 33＝26，17 mod 33＝1 和 57 mod 33＝14。接收方解密后得到的明文的数字是 19、21、26、1 和 14，对应的字母是 S、U、Z、A 和 N。

上述的加密和解密过程可以用表 3.1 表示。

3. RSA 算法的安全性

RSA 算法的加密过程要求 n 和 k，解密过程要求 n 和 k'。n 和 k 及算法都是公开的。现在已知 n 和 k 的情况下是否能很容易或很快求出 k' 是衡量 RSA 算法安全性的关键因素。

在已知 n 和 k 的情况下求 k' 的关键是对 n 的因式分解，找出 n 的两个素数 p 和 q。而对算法的安全，就必须选择大的 n，也就意味着密钥要足够长。

表 3.1 RSA 算法的加密和解密过程

发送方计算机				接收方计算机		
明文		P^3	密文	E^7	解密	
符号	数值		P^3 mod 33		E^7 mod 33	符号
S	19	6859	28	12492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	1	1	1	1	1	A
N	14	2744	5	78125	14	N

密钥越长，安全性也就越高，但相应的计算机运算速度也就越慢。由于高速计算机的出现，以前认为已经很具有安全性的 512bit 密钥长度已经不再满足人们的需要。1997 年，RSA 组织公布当时密钥长度的标准是个人使用 768bit 密钥，公司使用 1024bit 密钥，而一些非常重要的机构要使用 2048bit 密钥。

4. 对称和非对称数据加密技术的比较

对称数据加密技术和非对称数据加密技术的区别如表 3.2 所示。

表 3.2 对称数据加密技术和非对称数据加密技术的比较

项　　目	对称数据加密技术	非对称数据加密技术
密码个数	1 个	2 个
算法速度	较快	较慢
算法对称性	对称，解密密钥可以从加密密钥中推算出来	不对称，解密密钥不能从加密密钥中推算出来
主要应用领域	数据的加密和解密	对数据进行数字签名、确认、鉴定、密钥管理和数字封装等
典型算法实例	DES 等	RSA 等

3.3.3 PGP 加密软件简介

PGP(pretty good privacy)是一种操作简单、使用方便、普及程度较高的，基于不对称加密算法 RSA 公钥体系的邮件加密软件。PGP 不但可以对电子邮件加密，防止非授权阅读信件，还能对电子邮件附加数字签名，使收信人能明确了解发信人的真实身份，也可以在不需要通过任何保密渠道传递密钥的情况下，使人们安全地进行保密通信。

PGP 创造性地把 RSA 不对称加密算法的方便性和传统加密体系结合起来，在数字签名和密钥认证管理机制方面采用了无缝结合的巧妙设计，同时具有良好的人机工程设计。它功能强大，有很快的速度，而且是完全免费的。另外，PGP 还可以用来加密各种类型的文件，这些优势使其几乎成为最流行的公钥加密软件包。

PGP 实际上采用的是 IDEA 传统加密算法用来加密的，而不是 RSA 本身。原因是 RSA 算法计算量极大，在速度上不适合加密大量数据，而 IDEA 的加解密速度比 RSA 要快得多，所以实际上 PGP 是以一个随机生成的密钥，用 IDEA 算法对明文加密，然后再用 RSA 算法对该密钥进行加密的。收件人同样是用 RSA 解密这个随机密钥，再用 IDEA 解密邮件本身。这样的链式加密就做到了既有 RSA 体系的保密性，又有 IDEA 算法的快捷性。

PGP 不仅有加密的功能，还可以用于数字签名。用 PGP 进行数字签名的过程为：发送方用自己的私钥将 128bit 的特征值加密，附加在邮件后，再用接收方的公钥将整个邮件加密。在这里特别要注意次序，如果先加密再签名的话，别人可以将签名去掉后加上自己的签名，从而篡改了签名。密文收到以后，接收方用自己的私钥将邮件解密，得到发送方的原文和签名，然后用 PGP 从原文计算出一个 128bit 的特征值来和用发送方的公钥解密签名所得到的数进行比较，如果符合就说明这份邮件确实是发送方发来的。这样就使两个安全性要求都得到了满足。

PGP 还可以只签名而不加密，这适用于公开发表声明时，声明人为了证实自己的身份，可以用自己的私钥签名。这样就可以让收件人能确认发信人的身份，也可以防止发信人抵赖自己的声明。这一点在商业领域有很大的应用前途，它可以防止发信人抵赖和信件被中途篡改。



【案例】 数据加密软件 PGP 的使用

案例分析

PGP(pretty good privacy)是一种操作简单、使用方便、普及程度较高的，基于不对称加密算法 RSA 公钥体系的邮件加密软件。

操作环境

(1) 一台连上 Internet 的计算机。

(2) Windows XP/2003，Windows 7 操作系统，PGP 软件。

操作步骤

第 1 步 下载并安装 PGP 软件。

PGP 是一款免费英文软件，一般专业软件下载网站都提供下载。以 PGP 8.0.1 为例，经解压缩后，双击 PGP 8.0.1 安装文件，出现如图 3.18 所示的画面。

按照提示，反复单击“下一步”按钮，即可安装成功。重新启动计算机后，可在屏幕上显示 PGP 活动栏，如图 3.19 所示。

第 2 步 建立一对密钥的步骤。

单击 PGPkey 按钮，然后依次完成如下步骤。





图 3.18 PGP 的安装



图 3.19 PGP 活动栏

(1) 根据密钥生成向导，逐屏选择密钥的类型、密钥长度、密钥期限等。

(2) 设置私钥传递词，以保护私钥。

(3) 可以根据需要决定是否把密钥送到默认的服务器上。

(4) 保存密钥。

第 3 步 加密步骤。

为了有一个实验对象，先在 C:\下建立一个文件 PGPexecise.doc。

(1) 单击 Encrypt 按钮。在打开的 Select Files 对话框中选择要加密的文件，选定后单击“打开”按钮。

(2) 在 PGP key Selection Dialog 对话框中选取对方的公有密钥。

(3) 输入自己的私钥，将 PGPexecise.doc 转换为.pgp 文件。

第 4 步 解密步骤。

(1) 接收者输入自己的密钥，即可解密文件。

(2) 在 PGPLog 对话框中查看文件的签名状态。

3.4 数字签名

3.4.1 数字签名的定义

生活中，许多文件的真实性和可靠性最终要根据是否有亲笔签名来确定，复印件是无效的。如果要用计算机报文代替纸墨文件的传送，就必须找到解决亲笔签名的方法，这样，数字签名(digital signature)就应运而生了。如今，数字签名已经在诸如电子邮件、电子转账、办公室自动化等系统大量应用了。

数字签名是指信息发送者使用公开密钥算法的主要技术，产生别人无法伪造的一段数字串。发送者用自己的私有密钥加密数据后，传给接收者。接收者用发送者的公钥解开数据后，就可确定数据来自于谁。同时这也是对发送者发送的信息真实性的一个证明，发送者对所发送的信息是不能抵赖的。

数字签名用来保证信息传输过程中信息的完整和提供信息发送者的身份认证。例如，在电子商务中要求安全、方便地实现在线支付，而数据传输的安全性、完整性，身份验

证机制及交易的不可抵赖性等，大多是通过安全性认证手段加以解决的。数字签名可以进一步方便电子商务的开展。例如，商业用户无需在纸上签名或为信函往来而等待，足不出户就能够通过网络获得贷款、购买保险或者与房屋建筑商签订契约等。企业之间也能通过网上协商达成有法律效力的协议。

一个数字签名算法主要由两个算法组成，即签名算法和验证算法。签名者能使用一个秘密的签名算法签一个消息，所得的签名能通过一个公开的验证算法来验证。给定一个签名后，验证算法根据签名是否真实来做出一个“真”或“假”的问答。其过程可描述为：甲首先使用他的秘密密钥对消息进行签名得到加密文件，然后将文件发给乙，最后，乙用甲的公钥验证甲的签名的合法性。这样的签名是符合以下可靠性原则的。

（1）签名是可以被确认的。

（2）签名是无法被伪造的。

（3）签名是无法重复命名使用的。

（4）文件被签名以后是无法被篡改的。

（5）签名具有无可否认性。

目前已有大量的数字签名算法，如RSA数字签名算法、EIGamal签名算法、美国的数字签名标准/算法（DSS/DSA）、椭圆曲线数字签名算法和有限自动机数字签名算法等。

数字签名的保密性很大程度上依赖于公开密钥。数字签名的加密/解密过程和秘密密钥的加密/解密过程虽然都使用公开密钥体系，但实现的过程正好相反，使用的密钥对也不同。数字签名使用的是发送方的密钥时，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密。这是一个一对多的关系，任何拥有发送方公开窃钥的人都可以验证数字签名的正确性。而秘密密钥的加密/解密则使用的是接收方的密钥对，这是多对一的关系，任何知道接收方公开密钥的人都可以向接收方发送加密信息，只有唯一拥有接收方私有密钥的人才能对信息解密。这是一个复杂但又很有趣的过程。在实用过程中，通常一个用户拥有两个密钥对，一个密钥对用来对数字签名进行加密/解密，一个密钥对用来对秘密密钥进行加密/解密。这样的方式提供了更高的安全性。

由于加密密钥是公开的，所以密钥的分配和管理就很简单，而且能够很容易地实现数字签名。因此，非常适合于电子商务应用的需要。在实际应用中，公开密钥加密系统并没有完全取代秘密密钥加密系统，这是因为公开密钥加密系统的计算非常复杂，它的速度远赶不上秘密钥匙加密系统。因此，在实际应用中可利用二者的各自优点，采用秘密钥匙加密系统加密文件，采用公开密钥加密系统加密“加密文件”的密钥，这就是混合加密系统，它较好地解决了运算速度问题和密钥分配管理问题。

3.4.2 数字签名的应用

数字签名可以用对称算法实现，也可以用非对称算法实现，还可以用报文摘要算法实现。

1. 使用对称密钥算法进行数字签名

对称密钥算法所用的加密密钥和解密通常是相同的，即使不同也可以很容易地由其

中的一个推导出另一个。在此算法中，加密/解密双方所用的密钥都要保守秘密。由于其计算速度快，而广泛应用于大量数据的加密过程中。使用对称密钥密码算法进行数字签名的加密标准有 DES、RC2、RC4 等。

其签名和验证过程为：利用一组长度是报文的 bit 数 n 两倍的密钥 A 来产生对签名的验证信息，即随机选择 $2n$ 个数 B，由签名密钥对这 $2n$ 个数 B 进行一次加密交换，得到另一组 $2n$ 个数 C。发送方从报文分组的第一位开始依次检查，若为 0 时，取密钥 A 的第 1 位，若为 1 则取密钥 A 的第 2 位……直至报文全部检查完毕。所选取的 n 个密钥位形成了最后的签名。接收方对签名进行验证时，也是首先从第 1 位开始依次检查报文分组，如果它的第 x 位为 0 时，它就认为签名中的第 x 组信息是密钥 A 的第 x 位，若为 1 则为密钥 A 的第 $x+1$ 位，直至报文全部验证完毕，就得到了 n 个密钥。由于接收方具有发送方的验证信息 C，所以可以利用得到的 n 个密钥检验验证信息，从而确认报文是否是由发送方所发送。

由于这种方法是逐位进行签名的，所以只要有一位被改动过，接收方就得不到正确的数字签名，因此其安全性较好。其缺点是：签名太长，签名密钥及相应的验证信息不能重复使用，否则极不安全。

2. 使用非对称密钥密码算法进行数字签名

非对称密钥密码算法(即公钥密码算法)使用两个密钥：公开密钥和私有密钥，分别用于对数据的加密和解密，即如果用公开密钥对数据进行加密，只有用对应的私有密钥才能进行解密。如果用私有密钥对数据进行加密，则只有用对应的公开密钥才能解密。使用非对称密钥密码算法进行数字签名的加密标准有 RSA、DSA、Diffie-Hellman 等。

其签名和验证过程为：发送方首先用公开的单向函数对报文进行一次变换，得到数字签名，然后利用私有密钥对数字签名进行加密后，附在报文之后一同发出。接收方用发送方的公开密钥对数字签名进行解密交换，得到一个数字签名的明文。发送方的公钥可以由一个可信赖的技术管理机构，即认证中心(CA)发布。接收方将得到的明文通过单向函数进行计算，同样得到一个数字签名，再将两个数字签名进行对比。如果相同，则证明签名有效，否则无效。

这种方法使任何拥有发送方公开密钥的人都可以验证数字签名的正确性。由于发送方私有密钥的保密性，使接收方既可以根据结果来拒收该报文，也能使其无法伪造报文签名及对报文内容进行修改，原因是数字签名是对整个报文进行的，是一组代表报文特征的定长代码，同一个人对不同的报文将产生不同的数字签名。这就解决了银行通过网络传送一张支票，而接收方可能对支票数额进行改动的问题，也避免了发送方逃避责任的可能性。

3. 报文摘要算法

报文摘要是最主要的数字签名方法，也称为数字摘要法或数字指纹法。该数字签名方法是将数字签名与要发送的信息紧密联系在一起，它更适合电子商务活动。将一个报文内容与签名结合在一起，比内容和签名分开传递有着更强的可信度和安全性。使用报

文摘要算法进行数字签名的通用加密标准有 SHA-1、MD5 等。下面以 MD5 为例简要说明。

MD5 是目前应用最广泛的报文摘要算法，是一个可以为每个文件生成一个数字签名的工作。MD5 属于一种 Hash(哈希)函数，其定义为：算法以一个任意长信息作为输入，产生一个 128bit 的“指纹”或“摘要信息”。

MD5 算法对需要进行摘要处理的报文信息块按 512bit 处理。首先它对报文信息进行填充，使其长度等于 512 的倍数。填充的方法是在需要进行摘要处理的报文信息块后填充 64 字节长的信息长度，然后再用首位为 1，后面全为 0 的信息进行填充。然后对信息报文进行处理，每次处理 512bit，每次进行 4 轮(每轮 16 步，共 64 步)的信息变换处理，每次输出结果为 128bit，然后把前一次的输入作为下一次信息变换的输入初值，这样最后输出一个 128bit 的 Hash 摘要结果。目前 MD5 被认为是最安全的 Hash 算法之一，已经在很多应用中被当成标准来使用。

MD5 提供了一种单向的 Hash 函数，是一种校验工具。它将一个任意长的字串作为输入，产生一个 128bit 的“报文摘要”，附在信息报文后面，以防报文被篡改。MD5 被认为对两个不同报文产生相同的报文摘要是不可计算的，并且对一个已给定的报文摘要，对另一个报文产生同样的报文摘要也是不可计算的。

在计算机安全中，MD5 算法是非常有效的一种对付特洛伊木马程序的工具。通过 MD5 算法计算每个文件的数字签名可以检查文件是否被更换或是否与原来的一致。

4. 数字签名的发展方向

(1) 数字签名的不足

在实际应用中，数字签名还存在一些不足之处。

① 数字签名亟待相关法律条文的支持。需要立法机构对数字签名技术有足够的重视，并且在立法上加快脚步，迅速制定有关法律，以充分实现数字签名具有的特殊鉴别作用，有力地推动电子商务及其他网上事务的发展。

② 如果发送方的信息已经进行了数字签名，那么接收方就一定要有数字签名软件，这就要求软件具有很高的普及性。

③ 假设某人发送信息后，被取消了原有数字签名的权限，以往发送的数字签名在鉴定时只能在取消确认列表中找到原有确认信息，这样就需要鉴定中心结合时间信息进行鉴定。

④ 数字签名中的基础设施，如鉴定中心、在线存取数据库等的建设费用，可能会影响到这项技术的全面推广。

(2) 数字签名的发展方向

首先，现有的一些基于优良算法的数字签名还会有很大的发展，如基于大整数因子分解难题的 RSA 算法和基于椭圆曲线上离散对数计算难题的 ECC 算法等。

以后的加密、生成和验证数字签名的工具将不断完善，会建立广泛的协作机制来支持数字签名，这将是 Web 发展的目标。确保数据保密性、数据完整性和不可否认性才能保证电子商务的安全交易。今后，与数字签名有关的复杂认证能力将像现在应用环境中的

口令保护一样,直接做到操作系统环境、信息传递系统及 Internet 防火墙。

数字签名作为电子商务的应用技术,将越来越受到人们的重视。其中涉及的关键技术也很多,并且有很多新的协议,如网上交易安全协议 SSL、SET 协议都会涉及数字签名,究竟使用哪种算法、哪种 Hash 函数以及数字签名管理,在通信实体与可能有的第三方之间使用协议等问题都可以作为新的课题。相信,数字签名的前景将越来越广阔。

3.5 密钥管理

由于加密算法的分开,对明文的保密将主要依赖于密钥。一旦密钥丢失或出错,不仅合法用户不能提取信息,还可能会导致非法用户窃取信息。所以,密钥的安全管理在信息系统安全中是极为重要的。它不仅会影响系统的安全性,还会涉及系统的可靠性、有效性和经济性。

密钥管理包括密钥的产生、存储、装入、分配、保护、丢失、销毁等内容。其方法的选取是基于参与者对使用该方法的环境所做的评估的。对环境的考虑包括要进行防范所使用的技术,提供的密码服务的体系结构与定位,以及密码服务提供者的物理结构与定位。

1. 对称密钥的管理

对称加密是基于共同保守秘密来实现的。采用对称加密技术的通信双方必须要保证采用的是相同的密钥,要保证彼此密钥的交换是安全、可靠的,同时还要设定防止密钥泄密和更改密钥的程序。这样对称密钥的管理就会变成一件烦琐且充满潜在威胁的工作,解决的办法是通过公开密钥加密技术实现对称密钥的管理。这样将使相应的管理变得简单和更加安全,同时还解决了纯对称密钥模式中存在的可靠性问题和鉴别问题。

通信的一方可以为每次交换的信息生成唯一的一把对称密钥,并用公开密钥对该密钥进行加密,然后再将加密后的密钥和用该密钥加密的信息一起发送给相应的另一方。由于对每次信息交换都对应生成了唯一的一把密钥,因此,双方就不再需要对密钥进行维护和担心密钥的泄露或过期。这种方式的另一优点是,即使泄露了一把密钥也只将影响一次通信过程,而不会影响到双方之间所有的通信。同时,这种方式也提供了发布对称密钥的一种安全途径。

2. 公开密钥的管理

通信双方可以使用数字证书(公开密钥证书)来交换公开密钥。国际电信联盟制定的标准 X.509 对数字证书进行了定义。该标准等同于国际标准组织(ISO)与国际电工委员会(IEC)联合发布的 ISO/IEC 9594—8195 标准。数字证书通常包含唯一标识证书所有者的名称、唯一标识证书发布者的名称、证书所有者的公开密钥、证书发布者的数字签名、证书的有效期及证书的序列号等。证书发布者一般称为证书管理机构(CA),它是通信双方都信赖的机构。数字证书能够起到标识通信双方的作用,是目前广泛采用的密钥管理技术之一。

3. 密钥管理的相关标准规范

目前国际有关的标准化机构都着手制定了关于密钥管理的技术标准规范。ISO 与 IEC 下属的信息技术委员会(JTC1)已起草了关于密钥管理的国际标准规范。该规范主要由三部分组成,第一部分是密钥管理框架,第二部分是采用对称技术的机制,第三部分是采用非对称技术的机制。该规范现已进入到国际标准草案表决阶段,并将很快成为正式的国际标准。

本章小结

加密是保护数据安全的一种最常用的方法。数据加密技术分为两种:传统加密方法和现代加密方法。传统加密方法的典型代表是替代密码和换位密码技术。现代加密方法的典型代表是 RSA 和 DES 加密方法。

数字签名是加密技术的典型应用,用来保证信息传输过程中信息的完整和提供信息发送者的身份认证。

本章练习

一、填空题

1. DES 使用的密钥长度是________位。

2. 有一类加密类型通常用于数据完整性检验和身份验证,例如,计算机系统中的口令就是利用________算法加密的。

3. 认证技术主要解决网络通信进程中通信双方________认可。

4. 电子商务中的数字签名通常利用公开密钥加密方法来实现,其中发送者签名使用的密钥为发送者的________。

5. 数字签名是用于确认发送者身份和消息完整性的一个加密的________。

6. PGP 软件不仅有________功能,还有________功能。这两种功能可能同时使用,也可以________使用。

二、选择题

1. 如果使用恺撒密码,在密钥为 4 时 attack 的密文为________。

   A. ATTACK　　B. DWWDFN　　C. EXXEGO　　D. FQQFAO

2. 按密钥的使用个数,密码系统可以分为________。

   A. 置换密码系统和易位密码系统　　B. 分组密码系统和序列密码系统

   C. 对称密码系统和非对称密码系统　　D. 密码学系统和密码分析学系统

3. 计算机网络系统中广泛使用的 DES 算法属于________。

   A. 不对称加密　　B. 对称加密　　C. 不可逆加密　　D. 公开密钥加密

4. 在公钥密码体系中,下面________是可以公开的。

Ⅰ. 加密算法　　Ⅱ. 公钥　　Ⅲ. 私钥

A. 仅Ⅰ　　B. 仅Ⅱ　　C. 仅Ⅰ和Ⅱ　　D. 全部

5. 关于数字签名,下面说法错误的是________。

A. 数字签名技术能够保证信息传输过程中的安全性

B. 数字签名技术能够保证信息传输过程中的完整性

C. 数字签名技术能够对发送者的身份进行认证

D. 数字签名技术能够防止交易中抵赖的发生

三、简答题

1. 简述密码技术的概念。
2. 简要描述传统的加密方法。
3. 简述 DES 算法 16 个子密钥的生成过程。
4. 公开密钥体制 RSA 算法的主要特点是什么?
5. 试说明数字签名实现的过程。
6. PGP 软件的功能是什么? 可应用在什么情况下?

实训　PGP 非对称加密应用

实训目的

(1) 掌握文件的机密性保护方法。

(2) 掌握对保护文件提供完整保护方法。

(3) 掌握对称与非对称加密综合应用方法。

实训环境

(1) PGP 安装软件,Apocalypso 安装软件。

(2) 局域网。

实训步骤

第 1 步　PGP 软件的安装。

(1) 解压缩后,双击或运行安装程序后,进入安装界面,显示欢迎信息,单击 Next 按钮,出现许可协议说明,阅读后选择接受,进入提示安装 PGP 所需要的系统及软件配置情况的界面,继续单击 Next 按钮,出现创建用户类型的界面,单击 Next 按钮。

(2) 安装程序会提示用户,是否已经有了密钥,如果安装过 PGP 计算机中可能存在密钥,这就可以再利用了。如果没有安装过 PGP 则选择 No I'm a new user,然后单击 Next 按钮出现程序的安装目录,建议将 PGP 安装程序默认的目录,也就是系统盘内,程

序很小，再次单击 Next 按钮，出现选择 PGP 组件的窗口，安装程序会检测系统内所安装的程序，如果存在 PGP 可以支持的程序，它将自动选中该支持组件，如图 3.20 所示。PGP 可以和 Outlook 结合完成邮件的加密。

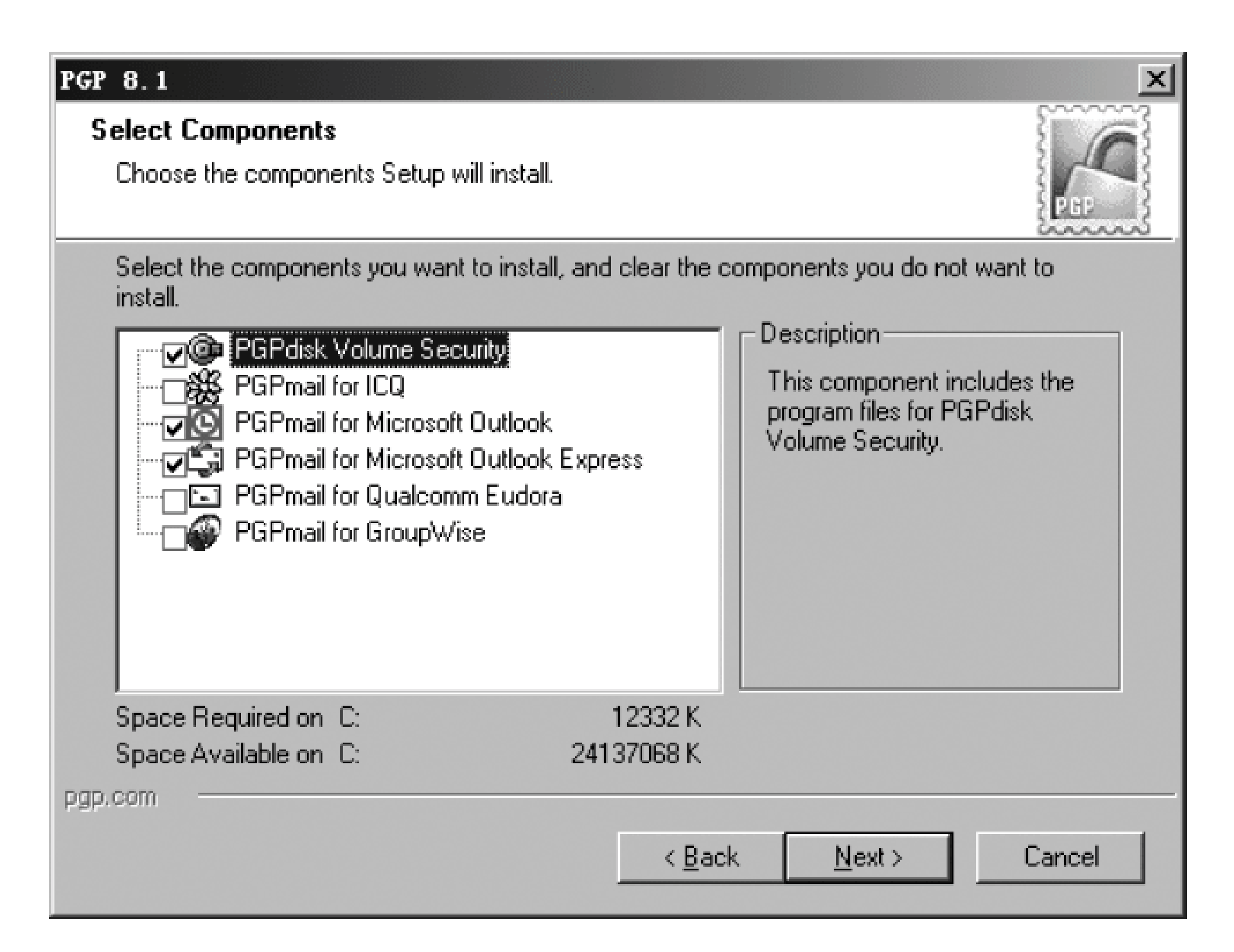


图 3.20 PGP 组件窗口

(3) 最后安装过程按提示单击 Next 按钮，最后提示重启系统即可完成安装。重启系统之后，系统会启动 PGP 许可验证，PGP 已经在"开始"→"所有程序"→"启动"选项中加入启动项。输入购买时的产品相关许可码等信息，也可以选择试用模式，即选择 Later。

第 2 步 密钥对(公钥和私钥)的生成。

(1) 安装完成后会出现密钥生成向导，单击"下一步"按钮后要求输入用户全名和邮件地址，接下来会提示要求输入用于保护私钥的密码，此密码不能少于 8 位，并要求重复确认一遍。在 Passphrase 文本框输入需要的密码，Confirmation(确认)文本框再输入一次密码，密码的长度必须大于 8 位，建议为 12 位以上。

(2) 接下来进入 Key Gemeration Progress(密钥生成阶段)等待主密钥(Key)和次密钥(Subkey)生成完毕(Done)。单击 Next 按钮，进入 Completing the PGP Key Generation Wizard(完成该 PGP 密钥生成向导)界面，单击 Finish 按钮，完成密钥创建和设置，如图 3.21 所示。

第 3 步 密钥的查看。

通过开始程序中的 PGP 中启动 PGPKeys，可以看到密钥的一些基本信息，如 Trust Model(信任度)、Size(大小)、ID(密钥 ID)、Created(创建时间)、Expires(到期时间)等，如图 3.22 所示。

第 4 步 重新创建密钥对。

通过 PGP 程序窗口中的 Keys 菜单，可以重新生成另外一对密钥，如图 3.23 所示。

第 5 步 导出并发布自己的公钥。

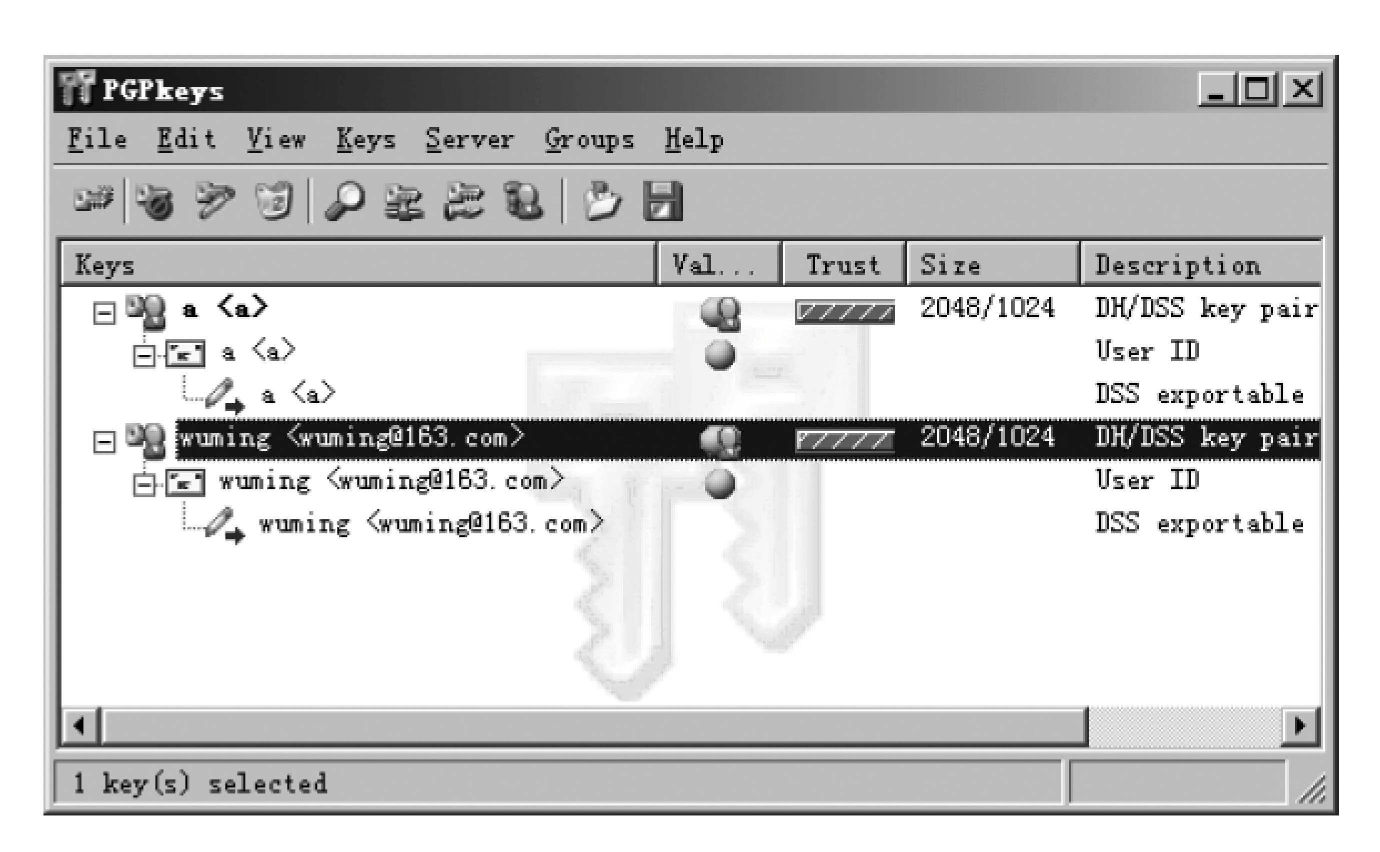


图 3.21　创建的密钥

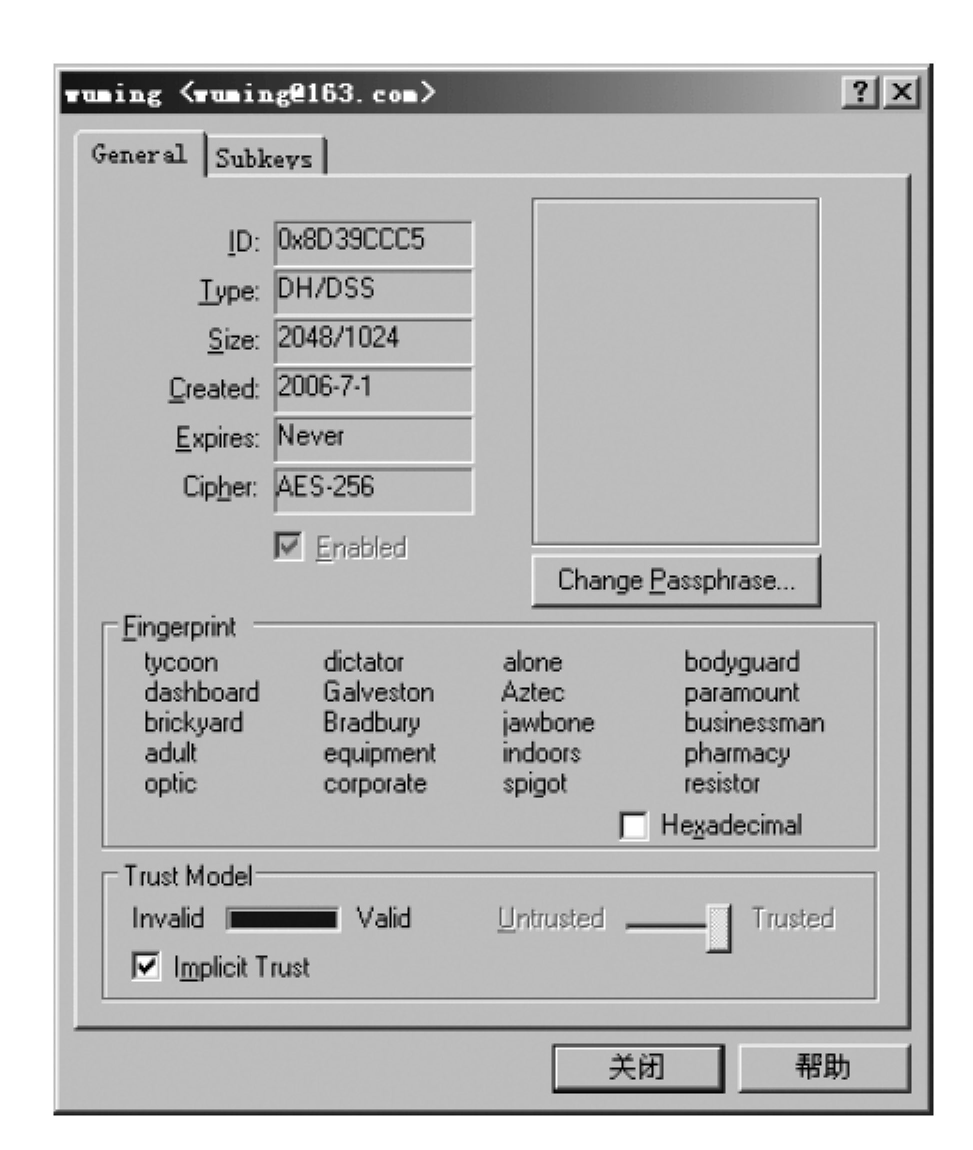


图 3.22　密钥基本信息

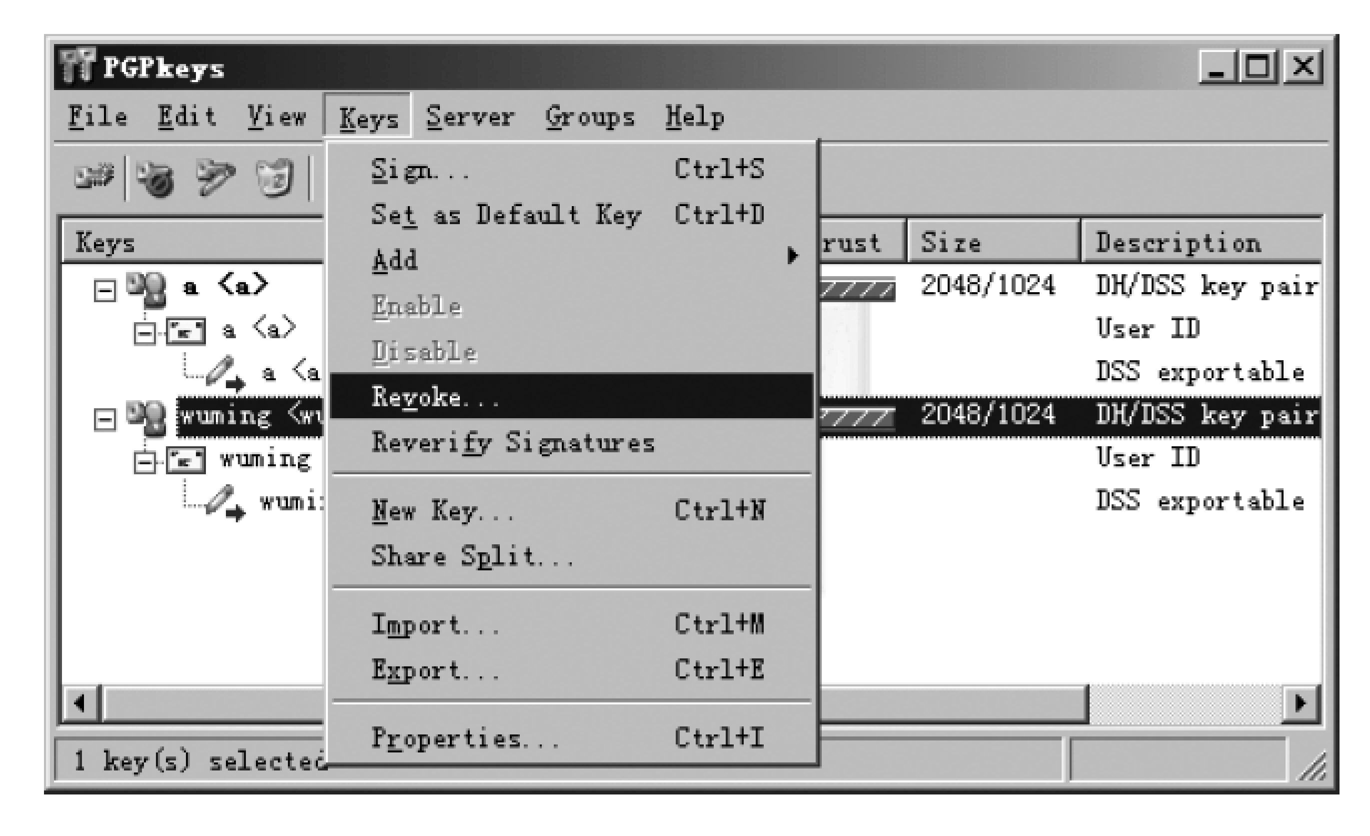


图 3.23　生成另外一对密钥

通过 PGP 程序窗口中的 Keys 菜单，选择 Export 命令可以导出当前选中密钥中的公钥(如果在导出到文件窗口下面选中 Include Private Key 复选框则将导出公钥和私钥，一般情况下不需要导出私钥)，如图 3.24 所示。



图 3.24　导出公钥和私钥

第 6 步　导入并设置其他人的公钥。

可以从网上如 FTP 下获取对方的公钥，导入公钥：直接单击对方发来的扩展名为.Asc的公钥将会出现选择公钥的窗口，在这里可看到该公钥的基本属性，如有效性、创建时间、信任度等，便于了解是否应该导入此公钥。选好后，单击 Import 按钮，即可导入 PGP。打开 PGPKeys，就能在密钥列表里看到刚才导入的密钥。

第 7 步　利用 PGP 实施加密、验证与签名。

第 4 章 Windows Server 2003 的安全

Chapter 4

知识目标

- 了解操作系统的安全性。
- 掌握 Windows Server 2003 的用户管理及管理策略。
- 掌握 Windows Server 2003 的文件访问权限及管理策略。
- 掌握 Windows Server 2003 的资源审计方法。

技能目标

- 能够对 Windows Server 2003 中的用户管理及管理策略进行设置。
- 能够对 Windows Server 2003 的文件访问权限及管理策略进行设置。
- 能够对 Windows Server 2003 中的资源进行安全审计。

Windows Server 2003 已经成为目前 Windows 主流服务平台。本章主要以 Windows Server 2003 为主，介绍与 Windows Server 2003 系统有关的安全机制以及涉及 Windows Server 2003 系统安全的一些技巧。

4.1 操作系统安全简介

Windows 一直被认为是一个不安全的操作系统，它的安全性要远低于 Linux、UNIX 等操作系统。实际上，安全性与易用性通常是相对的，为了增强安全性，往往要牺牲一些易用性，而为了增强易用性，也往往要牺牲一些安全性。Windows 系统本身提供了不亚于其他操作系统的各项安全措施。只是为使用上和管理上的方便，这些安全措施在很多默认的情况下都没有开启，而 UNIX 的操作系统在默认安全性方面则比较出色。

决定系统安全的不是操作系统的类型，而是人，也就是说，是系统管理员的能力决定了一个系统的安全性而不是系统的类型。一个优秀的 Windows 系统管理员配置出来的 Windows 服务器要比一个水平差的 UNIX 管理员配置的 UNIX 系统要安全得多。只要有合理的配置，Windows 同样能提供非常高的安全性，能在各种各样要求高的应用中工作。

4.1.1 网络操作系统安全

1. 系统安全

不允许未经核准的用户进入系统，从而可以防止他人非法使用系统的资源是系统安全管理的任务。主要采用的手段有注册和登录。注册是指系统设置一张注册表，记录了注册的用户名和口令等信息，使系统管理员能掌握进入系统的用户情况，并保证用户名在系统中的唯一性。登录则是指用户每次使用系统时都要登录，通过核对用户和口令，核查该用户的合法性。同时，也可根据用户占用资源情况进行收费。

2. 用户安全

在操作系统中，用户对文件访问权限的大小，是根据用户分类、需求和文件属性来分配的。用户安全管理是为用户分配文件“访问权限”而设计的。可以对文件定义建立、删除、打开、读、写、查询和修改的访问权限。

3. 资源安全

资源安全是通过系统管理员或授权的资源用户对资源属性的设置，来控制用户对文件、打印机等的访问。可以设置执行、隐含、修改、索引、只读、写入、共享等属性。

4. 通信网络安全

通信网络中信息有存储、处理和传输 3 个主要操作，其中信息在传输过程中受到的安全威胁最大。因此，网络操作系统必须采用多种安全措施和手段，其主要内容如下。

(1) 用户身份验证和对等实体鉴别。远程录入用户和口令应当加密，密钥必须每次变更，以防被人截获后冒名顶替。对等实体鉴别是指在网络环境下，一个用户向另一个用户发送数据，发送方必须鉴别接收方是否确定是他要发送信息的人，接收方也要判别所发来的信息是否确定是由发送者本人发来的。

(2) 访问控制。指对哪些网络用户可访问哪些本地资源，以及哪些本地用户可访问哪些网络资源进行控制。

(3) 数据完整性。防止信息在传送和存储过程中的篡改、替换、删除等。

(4) 防抵赖。防止收发信息双方抵赖纠纷。发送方不能否认曾向接收方发送过信息，并且不否认接收方收到的信息是未被篡改过的原样信息。发送方也会要求收方不能在收到信息后抵赖或否认。

(5) 审计。主要审计用户对本地主机的使用和网络运行情况。

4.1.2 网络操作系统安全机制与安全策略

网络操作系统的安全机制主要有身份鉴别机制、访问控制、授权机制和加密机制。

1. 网络操作系统安全机制

(1) 身份鉴别机制

身份鉴别机制是大多数保护机制的基础，分为内部和外部身份鉴别两种。

① 外部身份鉴别是为了验证用户登录系统的合法性。一个合法的用户在其所能访问的系统中有一个用户账户，用户账户包括用户的用户名、口令及个人资料等一些基本信息。在这些信息中，账户可能是广为人知的，例如，它可能被用作一个电子邮件地址，而口令则对使用此账户的人员保密，此口令作为一个实体，只能被此账户的拥有者或系统管理员改变。当用户登录系统时，身份鉴别机制将验证用户身份，以确定该用户是否为合法的注册用户，并且确保不存在通过某些隐蔽的方式绕过系统验证机制进入系统。例如，某用户用一个用户名登录了某系统，此系统的外部身份鉴别机制将进行检查，以证实此登录用户确实是系统中拥有此用户名的用户。

外部身份鉴别的关键是口令的保密。口令一般是由字母、数字、特定符号等组成的字符串。口令的验证实现简单，理论上也比较可靠，但由于口令的验证在实现时需要人为配合，使安全性受到一定的影响。尽管对口令的安全还有争论，但口令仍然是近年来计算机及其网络访问控制的常驻机构用于身份鉴别的工具。

② 内部身份鉴别机制用于确保进程身份的合法性。若没有内部验证，某用户可以创建一个看上去属于另一用户的进程。从而使得即使是最有效的外部验证机制，在也会因为把这个用户的伪造进程看成另一个合法用户的进程而被轻易地绕过。

(2) 访问控制和授权机制

访问控制是操作系统安全机制最核心的内容。访问控制是确定谁能访问系统(关于鉴别用户和进程)、能访问系统何种资源(关于访问控制)及在何种程度上使用这些资源(关于授权)。访问控制包括对系统各种资源的存取控制，既包括对设备(如内存、虚拟存储器或磁盘等外存储器)的存取控制，也包括对文件、数据的存取控制。

① 授权。规定系统可以给哪些主体(subject)访问何种客体(object)的特权。授权机制确认用户或进程只有在策略许可时，才能够使用计算机的实体(如资源)。授权机制依赖于安全的验证机制而存在。

主体是一种能访问对象的活动实体，如人、进程或设备，它可以使信息在客体间流动。所以，对文件进行操作的用户是一种主体，用户调度并运行的某个作业也是一种主体。客体是含有或接收信息的实体，不受所依存的系统的限制。它可以是记录、数据块、存储页、存储段、文件、目录、目录树、信息树、信息和程序等，也可以是位、字节、域、处理器、通信线路或网络节点等。

对用户的授权一般可分成 4 种等级：超级用户、系统用户、普通用户和低级用户。在这 4 种特权等级中，超级用户的权力最大，低级用户的权力最小。

② 确定访问权限，并授权和实施。即规定以读或写，或执行，或增加，或删除的方式进行访问，并规定可以在何种程序使用系统的这些资源和实施访问。

(3) 加密机制

加密是将信息编码成像密文一样难解形式的技术，在现代计算机系统中，加密是整个

信息安全的理论和技术基础。在通过网络互联的计算机系统中，想要提供一种信息不可见的机制是困难的。因此，信息被加密成若不解密则其信息内容就是不可见的形式。加密的关键在于能高效地建立从根本上不可能被未授权用户解密的加密算法。

2. 网络操作系统安全策略

安全策略是根据组织现实要求所制定的一组经授权使用计算机及其信息资源的规则，它的目标是将信息安全事故的影响降为最小，保证业务的持续性，保护组织的资源，防范所有的威胁。

在操作系统中，各种安全管理方法的执行和安全机制的实施都来源于安全策略的制定。口令策略、访问控制与授权策略、审计策略等都是安全管理的依据所在。

(1) 口令策略

为保护口令，需研究口令的选择规律，剔除易被猜中的口令，可采取口令控制、口令检查、口令安全存储的技术。

① 口令的控制。可通过口令的使用、存储和改变，实施一定的控制来进行保护。

口令不允许显示，大多数系统在用户注册前后显示出一条信息，这些信息可帮助系统识别，并可为攻击者访问系统而提供输入信息的线索。系统应向系统管理员提供取消这些显示的功能。

- 限制措施。一些系统限制注册失败的次数，一般为 3 次或 6 次。当达到极限时，系统将该用户锁在外面，拒绝其注册。要记录注册失败的用户，以便跟踪。
- 口令的更换。每个口令有一定的使用期限，过此期限后，口令必须更换。
- 双口令系统。某些系统要求采用两个口令来存取敏感信息。先在注册时使用一个口令，用户在访问某些敏感信息时，系统要用户输入另一个口令，验证后才能决定是否允许访问。
- 最短口令长度，为防止口令被猜中，许多系统要求口令必须有一个最短长度限制。通常要求口令至少为 6～8 个字符长。
- 用户被锁。系统管理员可将规定时间之外使用 ID 和超过规定时间未改变口令的用户锁闭在外。
- 根口令保护。根口令是为鉴别系统管理员所唯一配置的。因为系统管理员比其他用户权限大，因此成为闯入者攻击的主要目标，应注意保护。

② 口令的检查。口令的检查有两种方法。第一种方法是按一定的时间间隔运行一个程序来检查。它可以比较现存的口令，以避免易猜中的口令。还可以取消已发现的易猜中口令，并通知用户在下次注册时改变它。第二种方法是当用户第一次输入口令时，系统通过执行一个算法来检查口令。

③ 口令的安全存储。口令通常以表格或清单的形式存储。这些存储信息包含了每一授权用户的口令。通常，系统收到一个用户发出的口令后，首先加密，接着系统再从口令数据库中取出该用户的加密口令，进行比较，如符合，则允许该用户在系统上注册，否则拒绝该用户注册。

(2) 访问控制与授权策略

访问控制策略是根据系统安全保密要求及实际可能而提出的一系列安全控制方法和策略。

(3) 系统监控和审计策略

未被发现的未经授权活动会导致重复的滥用,因此,应采取适当的措施对信息系统访问与使用活动进行监控,记录可监控事件,万一有安全事件发生,能提供客观证据。对监控的结果要进行检查。监控和审计策略包括以下内容。

① 建立并保存事件记录。建立审计日志以记录异常情况和其他有关的安全事件;规定审计日志的保留时间,以便支持将来调查和访问控制监督。

② 对系统使用情况进行监控。为确定用户只进行被明确授权的活动,要建立信息处理设施使用的监控程序,对信息处理设施的使用情况进行监控,发现问题及时采取安全措施。

4.1.3 操作系统的漏洞和威胁

虽然现代操作系统的安全机制比较完善,但是,由于系统设计的缺陷、系统配置的不合理性、安全策略的漏洞等,还是经常产生对操作系统的攻击。主要表现在以下几个方面。

(1) 以操作系统为手段,获得授权以外或未授权的信息。它危害计算机及其信息系统的保密性和完整性。如"特洛伊木马"、"逻辑炸弹"等都是如此。

(2) 以操作系统为手段,阻碍计算机系统的正常运行或用户的正常使用。它危害了计算机系统的可用性。例如,计算机病毒具有隐蔽性,又具有很强的再生机制和破坏性,可以使系统感染,也可以使应用程序或数据文件受到感染,造成程序和数据文件丢失或破坏,轻则占用系统资源,重则使系统瘫痪或崩溃。

(3) 以操作系统为对象,破坏系统完成指定的功能。除了计算机病毒破坏系统运行和用户正常使用外,还有一些人为因素,如干扰、设备故障和误操作也会影响软件的正常运行。

(4) 以软件为对象,非法复制和非法使用。

(5) 以操作系统为手段,破坏计算机及其信息系统的安全,窃听或非法获取系统的信息。



【案例】 IPC$ 远程入侵与防范

案例分析

本案例介绍如何建立和断开 IPC $ 连接,看看入侵者是如何将远程磁盘映射到本地的。通过 IPC $ 连接进行入侵的条件是已获得目标主机管理员的账号和密码,同时,也介绍了防范方法。

操作环境

（1）一台连上 Internet 的计算机。

（2）Windows 2003 系统。

操作步骤

第 1 步 选择“开始”→“运行”命令，在“运行”对话框中输入 cmd 命令，如图 4.1 所示。



图 4.1 “运行”对话框

第 2 步 建立 IPC $ 连接。

输入“net use \\192.168.1.108\ipc $ ”命令，如图 4.2 所示。

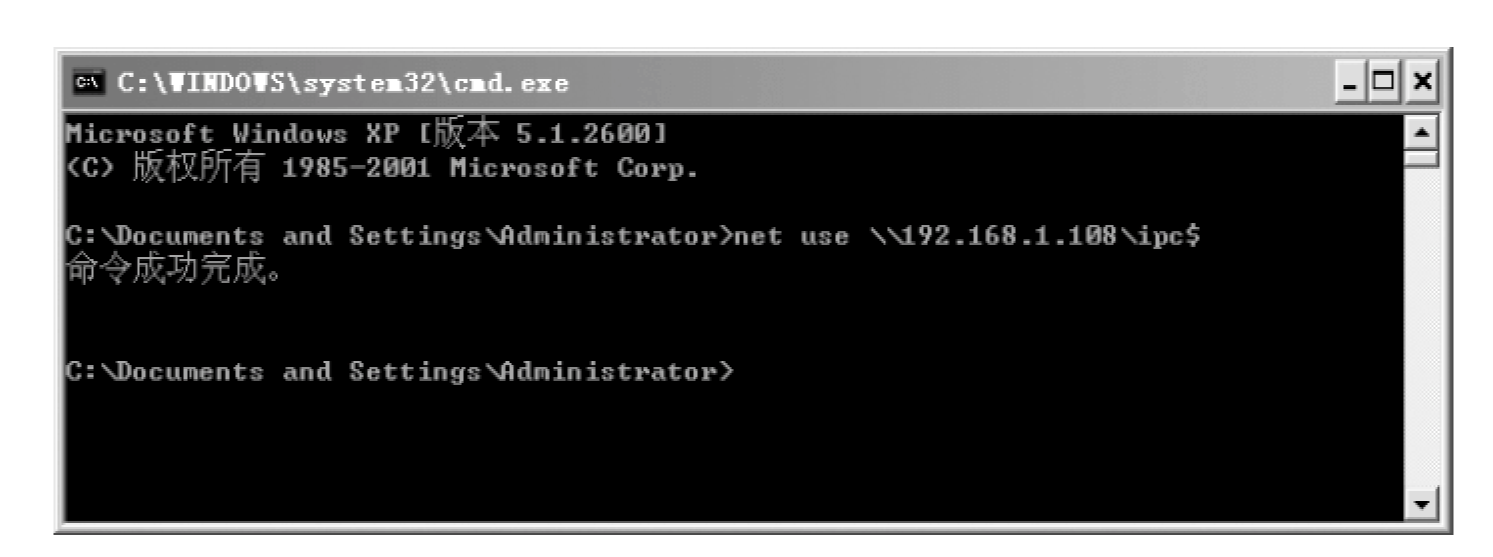


图 4.2 建立 IPC $ 连接

第 3 步 映射网络驱动器。使用如下命令。

```
net use z: \\192.168.1.108\c$
```

其中，“\\192.168.1.108\c $ ”表示目标主机 192.168.1.108 上的 C 盘，“ $ ”符号表示隐藏的共享，“z:”表示将远程主机的 C 盘映射为本地磁盘的盘符。该命令表示把 192.168.1.108 这台目标主机上的 C 盘映射为本地的 Z 盘，如图 4.3 所示。

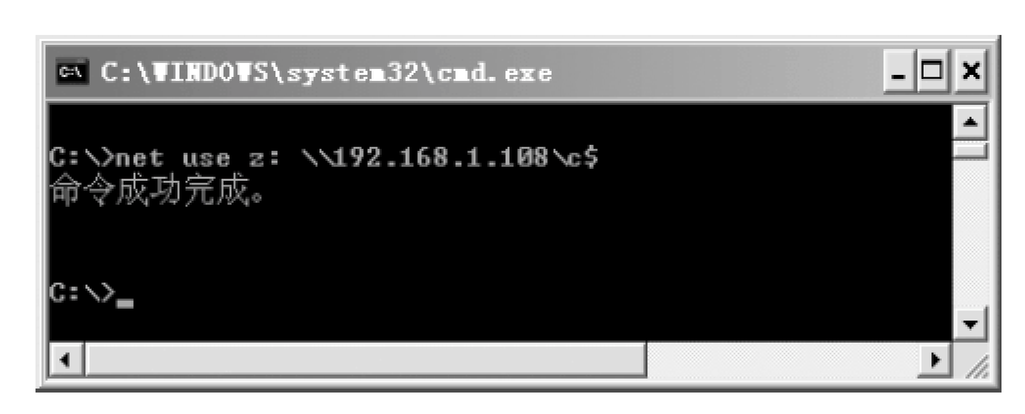


图 4.3 映射网络驱动器

映射成功后，打开“我的电脑”，会发现多出一个Z盘，上面写着“192.168.1.108上的c＄”，该磁盘即为目标主机的C盘，如图4.4所示。



图4.4　映射后的磁盘

第4步　查找指定文件。

右击Z盘，在快捷菜单中选择“搜索”命令，查找关键字“账目”，等待一段时间后，会得到结果，如图4.5所示。

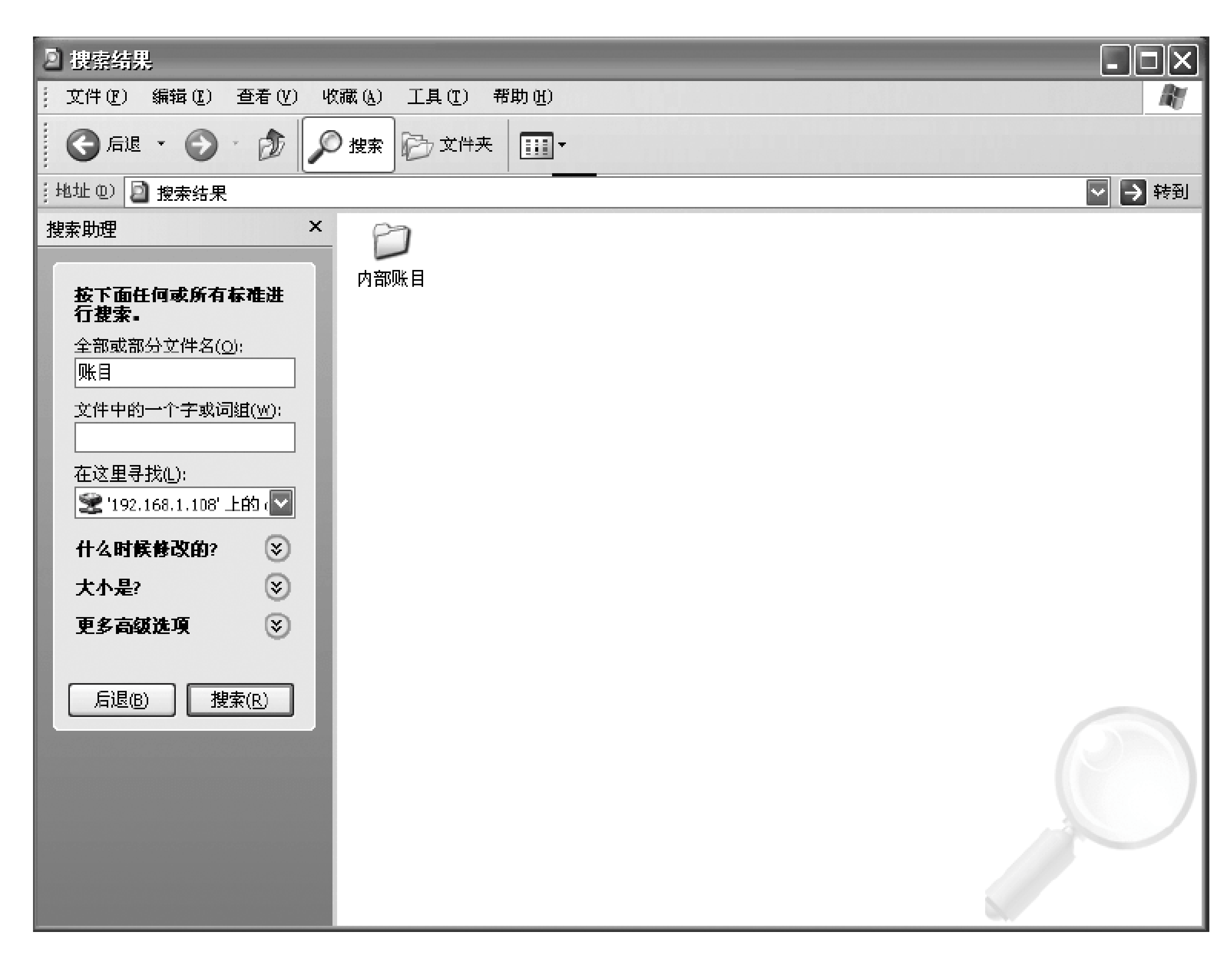


图4.5　搜索结果

然后将该文件复制、粘贴到本地磁盘，其复制、粘贴操作就像对本地磁盘进行操作一样。

第 5 步 断开连接。

输入“net use * /del”命令可断开所有的 IPC$ 连接。其中，“*”表示所有的连接，“/del”表示删除，如图 4.6 所示。

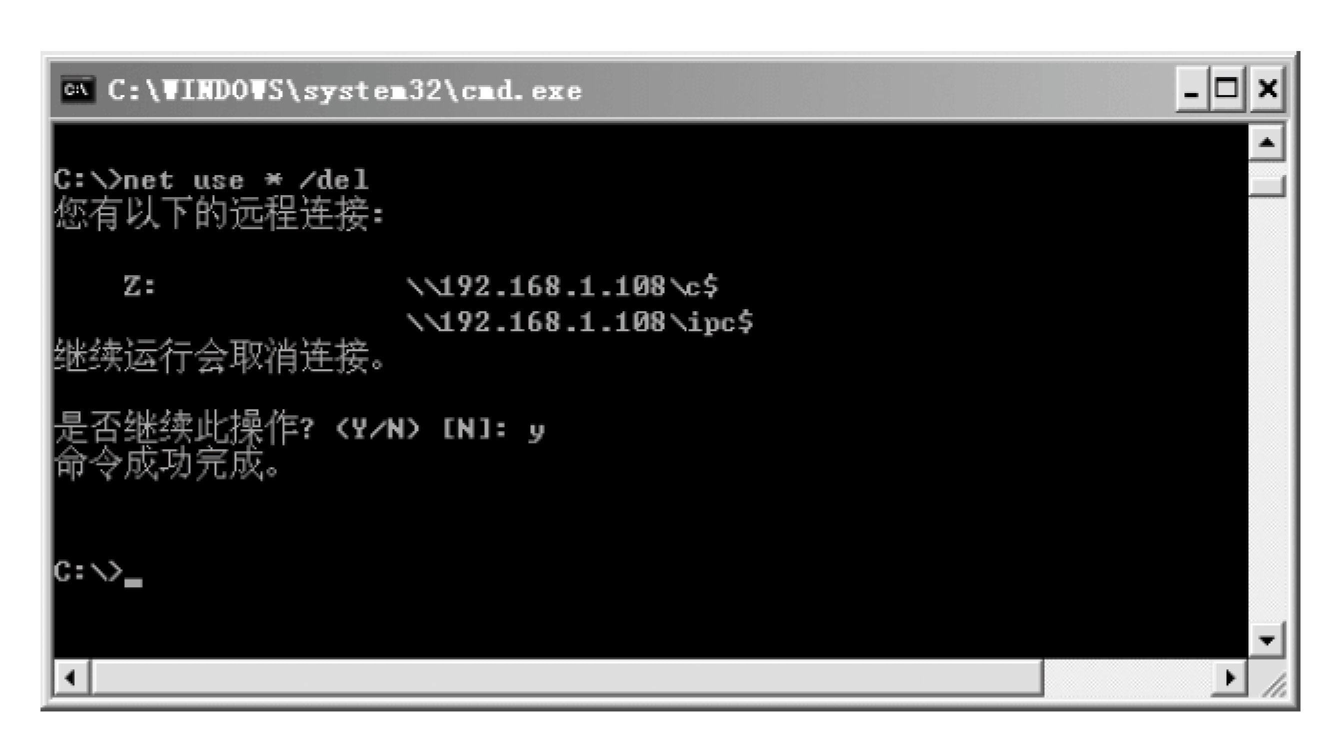


图 4.6 断开所有的 IPC$ 连接

另外，通过命令格式“net use \\目标 IP\共享名 /del”，可以删除指定目标 IP 的远程连接，如图 4.7 所示。

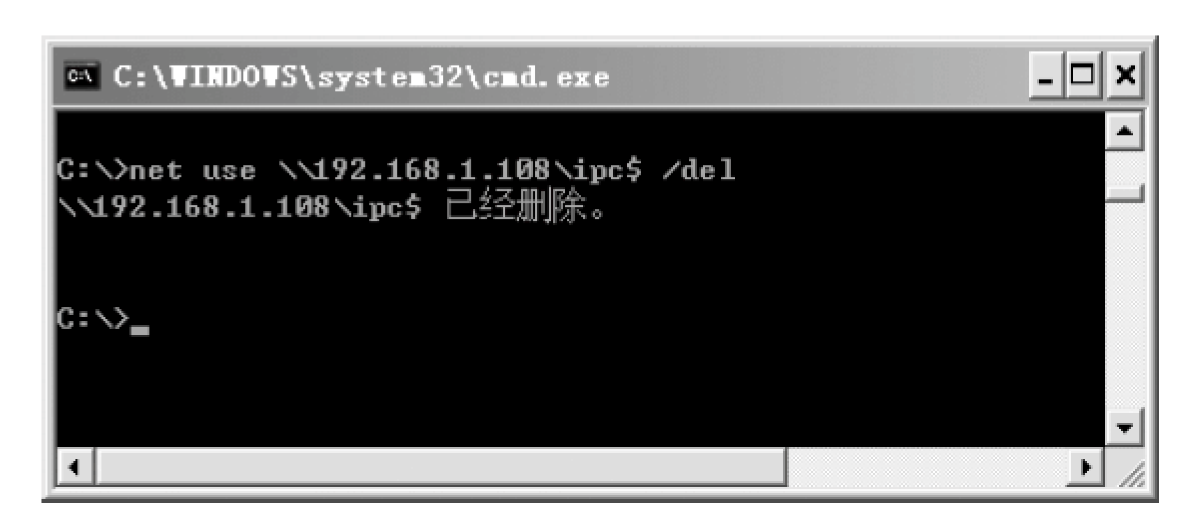


图 4.7 删除指定目标 IP 的远程连接

第 6 步 防范方法是首先要了解本机共享资源。

输入“net share”命令，查看本机共享资源。

第 7 步 通过 BAT 文件执行删除共享资源命令。

首先建立 BAT 文件，如建立的 BAT 文件为 noshare.bat，输入如下内容。

```
net share ipc$  /del
net share admin$  /del
net share c$  /del
net share d$  /del
```

如果有其他盘符，可以继续添加。然后将该文件保存后，拷贝至本机“开始”→“程序”→“启动”命令中。以后每次开机都会自动执行该 BAT 文件来删除默认共享。如果需要使用默认共享资源，则使用命令 net share 来打开共享，如使用“net share IPC$”命令来打开 IPC$。

4.1.4 Windows Server 2003

在微软的企业级操作系统中，如果说 Windows 2000 全面继承了 NT 技术，那么 Windows Server 2003 则是依据.NET 架构对 NT 技术进行了重要的发展和实质性的改进，并部分实现了.NET 战略，构筑了.NET 战略中最基础的一环。Windows 2003 Server 作为.NET 架构提出以来最重要、最基础性的产品，它的推出受到了业内人士的关注。

Windows Server 2003 简体中文版分 Web、Standard、Enterprise 和 Datacenter 4 个版本。Enterprise 版最大支持 8 个处理器和 32GB 内存，最小配置为 CPU 速度不低于 133MHz，内存不少于 128MB。因此，Windows Server 2003 具有硬件适应广和伸缩性强的特点。

Windows Server 2003 不仅改进了 Windows 2000 原有的服务，提高了这些服务的性能和扩充了许多功能，还增加了新的服务。

1. 安全性

原来的 Windows 系统的安全性总是不尽如人意，直到 Windows 2000 才有较大的改观，但依然存在缺憾，如登录时的输入法漏洞、IIS 特殊网址漏洞等。Windows Server 2003 在安全性上下了很大功夫，不仅堵住了已发现的 NT 漏洞，而且重新设计了安全子系统，增加了新的安全认证，改进了安全算法。

在本地安全策略方面，Windows Server 2003 区别于 Windows 2000 之处在于软件限制策略(SRP)。Windows Server 2003 允许用户控制在本地计算机系统上运行哪些软件。用户可在选项中规定系统要运行的软件，因此可阻止不被信任的软件运行。用户可定义默认的安全级别“允许未明确拒绝的”或“拒绝未明确允许的”。后来有较好的安全级别，但限制过于严格。

在用户组策略方面，Windows Server 2003 系统的组策略中增加了两项内容：软件限制策略(SRP)和无线网络策略(IEEE 802.11)。软件限制策略的功能与本地安全策略相同，但它可应用到站点、域或机构单位(OU)。无线网络策略允许管理员管理无线网络，定义优先的无线网络，并对任何系统定义 IEEE 802.1X 身份验证。

Windows Server 2003 的安全中心是活动目录(AD)。它集成了最新版本的 Windows 操作系统中的目录服务。Windows Server 2003 的活动目录较 Windows 2000 的活动目录的灵活和可管理性更强，可以处理森林域信任关系。

2. 可管理性

Windows Server 2003 的可管理性较 Windows 2000 有了很大提高，主要体现在各种服务的配置上。利用“配置您的服务器”和“管理您的服务器”向导，系统管理员可以轻松地进行服务器角色的安装和管理，从而完成各种服务器的安装和配置，其简单、方便和全面均非 Windows 2000 可比。Windows Server 2003 已内置了文件服务器、打印服务器、应用程序服务器、邮件服务器、终端服务器、远程访问/VTP 服务器、域控制器、DNS 服务

器、DHCP 服务器、流式媒体服务器、WINS 服务器等服务器角色,几乎囊括了所有的服务器应用。利用这些内置的服务器角色,只需简单的操作即可完成相应服务器的配置。用户还可以利用"管理您的服务器"对流媒体服务器的一些参数和选项进行调整。删除服务器也很简单,只需在"管理您的服务器"中删除相应的服务器角色即可。

3. 系统性能

通过实验测试,在相同的硬件配置下,Windows Server 2003 的启动速度和程序运行速度比 Windows Server 2003 要快许多,在低档硬件配置下和运行像 Photoshop 这类大型软件时表现得更明显。这无疑是 Windows Server 2003 核心得到改进、各种设备的管理得到优化的结果,同时也表明,Windows Server 2003 作为服务器操作系统有十分突出的内存管理、磁盘管理和线程管理性能。作为新一代网络操作系统,Windows Server 2003 有自己独有的设备管理模式,所以硬件驱动程序要安装"For Windows 2003"的产品,而且最好是经微软认证获得数字签名的产品,这样才能保证 Windows Server 2003 的稳定性和安全性。Windows Server 2003 已内置大多数主流硬件的程序,这些程序与硬件厂商提供的驱动程序相比,稳定性和兼容性都很好。

4. 安装和界面

Windows Server 2003 的安装类似于 Windows XP,区别是屏幕上角的 Windows Server 2003 提醒。安装分为升级安装和全新安装两种。Windows Server 2003 Enterprise 版只能从 Windows NT Server 4.0+SP5 或更高版本及 Windows 2000 Server 的各个版本升级。如果未达到上述版本,只能先升级到以上版本后再升级到 Windows Server 2003。

Windows Server 2003 已全面更换为 Windows XP 界面,同时也为习惯于传统 Windows 版本的操作者准备了传统的 Windows 界面。微软计划将所有产品的界面统一于 Windows XP 式样以适应.NET 战略,这在 Windows Server 2003 中得到了再次体现,也将在 Office 2003、Visual Studio.NET 2003 等产品中得到进一步的体现。

5. 功能

Windows Server 2003 改进并增强了如下功能。

(1) 远程控制功能。Windows Server 2003 增强了原来通过 Netmeeting 才能实现的"远程桌面连接",使系统管理员对网络的控制和管理大大加强。

(2).NET Framework 计算平台。为了适应.NET 战略,Windows Server 2003 提供了.NET Framework 计算平台,它简化了 Internet 分布式环境中应用程序的开发(如开发 ASP.NET 应用程序和 XML Web 服务),并为这些应用程序提供了良好的支持和缩放的服务端运行环境。

(3) IIS 6.0。Windows Server 2003 内置了 IIS 6.0 版,它较 Windows 2000 中的 IIS 5.0 在可靠性、安全性、可管理性等方面有了长足的进步,尤其是在全面支持.NET 架构上,提供了出色的 ASP.NET 运行环境和 Web 应用程序开发和运行机制。

(4) 流媒体服务。对流媒体服务器的改进,使微软作为流媒体技术领导者的地位得到进一步加强。流媒体服务器(Windows Media Player)版本已升至 9.0,它与客户端的 Windows Media Player 9.0 的配合非常密切。流媒体服务器改进了客户端和服务器的连接方式,使数据流在较差的网络环境下也能流畅地播放。流媒体服务器还提供了 SDK 开发包和各种调用接口,使程序开发人员可以定制和打造个性化的流媒体服务。

(5) 关闭事件跟踪功能。Windows Server 2003 在关机和重启模块中,增加了"关闭事件跟踪程序"选项,使用户在关机前进行选择。该功能对客户端无关紧要,但对服务器系统却很重要,因为服务器是连续工作的,非计划的关机或重启意味着事故,所以必须记录在案。

4.2 Windows Server 2003 安全性简介

Windows Server 2003 提供了一组全面的、可配置的安全性服务,安全性包括域控制器、文件服务器、Web 服务器、公共密钥和认证中心、防火墙及路由与远程服务等。

4.2.1 安全登录

Windows Server 2003 要求在允许用户访问系统之前,输入唯一的登录标识符和密码来标识自己。安全特性如下。

(1) 用户账户

要想登录 Windows Server 2003 域并访问计算机的资源及网络资源,就必须在 Windows Server 2003 系统中有自己的账户。每一个账户对应一个 Windows Server 2003 系统中的用户。

(2) 组

Windows Server 2003 默认定义一系列的组,并给这些组分配相应的权限,这些组的定义是为了方便实现对系统和用户的管理。

(3) Kerberos 身份验证协议

Kerberos 是 Windows Server 2003 默认的网络服务访问的认证机制,Kerberos 能解决旧的身份认证方式不能解决的很多问题。

4.2.2 访问控制

允许资源的所有者决定哪些用户可以访问资源和他们可以如何处理这些资源。所有者可以授权给某个用户或一组用户,允许他们进行各种访问。安全特性如下。

(1) 活动目录。活动目录是 Windows Server 2003 中最重要的特性之一。它将大大简化与执行和管理 Windows Server 2003 大型网络有关的任务,同时,它也将改善用户与网络资源间的交互性。为域提供了可升级的、灵活的账户管理,允许精确地访问控制和管理委托。

(2) NTFS 的权限。

(3) 共享文件访问许可。

(4) 分布式文件系统。

4.2.3 安全审计

提供检测和记录与安全性有关的任何创建、访问或删除系统资源的事件或尝试的能力。登录标识符记录所有用户的身份，这样便于跟踪任何执行非法操作的用户。

(1) 审计资源的使用。

(2) 监控网络资源的访问行为。

4.2.4 Windows Server 2003的安全策略

1. 安全策略概述

安全策略就是保证系统安全性的设置。安全策略可以应用到站点、域或组织单位，并影响到相关的用户组和计算机。设定组织的安全策略基于以下基本因素。

(1) 组织所选择实现的安全等级。这项特性决定了组织准备接受的风险量。

(2) 组织为安全操作所写的指南。它描述了管理员和用户为确保一个安全环境所应承受的责任。

(3) 为企业设计的活动目录名字空间。活动目录的层次结构名字空间决定了安全策略的作用域及哪些安全策略用于哪些组或计算机。

(4) Windows Server 2003 为活动目录安全策略和本地安全策略所做的设置。

安全策略按如下顺序应用。

① 唯一的本地组策略对象应用。

② 站点组策略对象，按照行政管理指定的顺序应用。

③ 域组策略对象，按照行政管理指定的顺序应用。

④ 对于组织单位组策略对象，按照从大组织单位到小组织单位顺序(从父组织单位到子组织单位)应用，而在每个组织单位级别中，则按照行政管理指定的顺序应用。

策略设置存储在组策略对象中，可以将组策略管理单元看成一个应用程序，因此，设置安全策略一般使用组策略对象。

有两种组策略对象：本地和域组策略对象。

存储在域控制器中的域策略对象只能在 Active Directory 环境下使用。它们适用于组策略对象所关联的站点、域或组织单位中的用户和计算机。

本地组策略对象存储在所有运行 Windows Server 2003 的计算机。一个本地组策略对象只能存储在一台计算机上，而且该对象在域组策略对象中有一个可用的设置子集。如果二者的设置发生冲突，域组策略对象的设置能覆盖本地组策略对象的设置。如果不发生冲突，则都可以应用。

2. Windows Server 2003 安全策略的内容

Windows Server 2003 安全策略主要包括 3 个方面，即本地组策略、域安全策略、域控制器安全策略。

(1) 本地组策略

使用这些对象,组策略设置可以存储在个人计算机上,无论这些计算机是否为 Active Directory 环境或网络环境的一部分。因为它的设置可以被与站点、域和单位关联的组策略对象覆盖,在 Active Directory 环境中,本地组策略对象的影响力最小。在非网络环境中(或缺少 Windows Server 2003 域控制器的网络环境中),本地组策略对象的设置比较重要,因为此时它们不能被其他组策略对象覆盖。本地策略的设置在"本地安全设置"窗口中进行,如图 4.8 所示。



图 4.8 本地安全设置

(2) 域安全策略和域控制器安全策略

域安全策略和域控制器安全策略应用于域内,针对站点、域或组织单位设置组策略,这些组策略的数据存储在活动目录内,即域控制器的%systemroot%\SYSVOL\sysvol\域名\policies 文件夹内。

域安全策略与域控制器安全策略的配置内容相似。

4.3 Windows Server 2003 的用户安全和管理策略

4.3.1 用户账户和组

在网络环境中,用户账户能为用户保留具有个性化的操作环境,如界面的设置(桌面、"开始"菜单、屏幕显示等)、鼠标和键盘的设置、输入法的设置、网络连接的设置等。但更为重要的是用来保证系统安全,防止用户非法使用计算机资源。

用户账号最重要的组成部分是用户名和密码。每个登录网络的用户必须要有用户账户。在登录到网络系统时,首先需要用户输入用户名和密码,然后系统对它们进行检查。在登录成功后,网络系统会根据管理员已赋予用户的权限来控制和监视用户对系统资源的访问。

1. 用户账户

(1) 用户账户的类型

在 Windows Server 2003 中有两种用户账户：本地用户账户和域用户账户。

① 建立在 Windows Server 2003 独立服务器、成员服务器或 Windows Server 2003 Professional 的本地计算机上的账户就是本地用户账户。通过本地用户账户，用户能够登录并访问本地计算机资源。但是只能访问这台计算机上的资源，无法访问网络上的资源。在 Windows Server 2003 中，"本地用户和组"及"用户和密码"管理器是用来管理本地用户和本地组的工具。

② 建立在域控制器的活动目录数据库中定义的账户就是域用户账户。通过域用户账户，用户能够登录到域并在网络上使用用户账户和密码，从任何计算机上访问域内资源。

(2) 内置用户账户

在网络操作系统安装完成后，安装程序自动创建了一些用户账户或用户对象，这些用户账户或用户对象为系统的配置、管理提供了基本的权利，这些用户账户或用户对象被称为内置用户账户。在安装 Windows Server 2003 时，安装程序自动创建了两种内置用户账户：一种是 Administrator（管理员）账户；另一种是 Guest（访客）账户。

① Administrator 账户拥有对计算机软件和网络设置的安全控制权，可以用它来管理计算机与域内的设置。如建立、更改或删除用户账户、设置安全策略，建立打印机、设置用户权限等。Administrator 可以被改名，但不能被删除、禁用或从 Administrator 本地组中撤销，从而保证用户不会因所有的管理级账户被删除或者失效而无法进入该计算机工作。这就是 Administrator 账户区别于其他 Administrator 本地组成员的主要特征。

② Guest 账户是供临时使用的账户，提供偶尔的登录或者为方便仅登录一次的用户使用。Guest 账户不需要设置密码。Guest 账户的默认值是禁用的，但管理员可以启用它。与任何用户账户一样，可以为 Guest 账户赋予各种权利和权限。在默认情况下，Guest 账户是内置 Guests 组的成员，它只允许用户从本地登录到工作站或成员服务器中，其他的权利及任何权限必须由管理员或账户操作员授予 Guest 本地组。

2. 组

组是用户账户的集合。通过组能够极大地简化用户账户的管理任务。例如，当为一个公司的成员创建用户账户时，必须对这些成员设置网络资源的使用权限，如果为每个账户分别设置权限，那将是烦琐并容易出错的。如果我们把这个公司的成员认为是一个组，只要把成员的账户加入到组中，再对组设置相关资源的权限，则每个成员的账户都拥有组的权限，这样就大大简化了用户的管理。

4.3.2 Windows Server 2003系统的用户账户的管理

1. 管理的基本内容

为使管理过程合理化和实现适当的安全措施，在管理用户账户时应考虑如下 6 个

问题。

(1) 命名约定

命名约定确立了在网络上如何识别用户。用户账户名称既是用户在网络上的唯一身份,又是用户登录网络或计算机系统的标识。

(2) 密码要求

用户账户的密码要求是为了保护对域或计算机资源的访问,也是对用户自身利益的保护。密码使用应遵循下述准则。

① 一定要给 Administrator 账户指定密码以防止未经授权的用户使用此账户。

② 告诉用户设法保护并经常变更其密码。设置密码时应遵循如下复杂性原则。

- 选择长密码。密码长度不要小于 6 位,密码越长,被猜中的可能性就越小。大多数系统密码设置为 5~8 个字符,还有许多系统允许更长的密码。
- 避免使用与用户有关联的信息。如家庭地址、电话号码或家庭成员的名字,以及生日、名字、年份或用户计算机中的典型特征等。同时,应避免在密码中使用用户账户名的任何部分。
- 密码中不要使用常用单词(避免字典攻击)或常用英文简称。
- 使用大写字符和小写字符混合编码。密码对字符的大小写是敏感的,如 PassWord 与 password 是不同的。
- 密码应该同时包含字母、数字、标点符号和控制字符。

③ 根据用户的工作性质,决定账户是否需要终止。对临时雇员,当他们的合同或工作契约结束时,终止他们的账户。

④ 设定控制密码的对象。密码控制有如下两种形式。

- 为用户分配唯一的密码并防止用户变更它,这是把控制权给予管理员。
- 为用户分配一个初始的密码,然后要求用户第一次登录时更改它,这是把控制权给予用户。

(3) 登录时间和站点限制

在默认情况下,拥有有效账户的用户可以每天 24 小时、每周 7 天内,从任何一台计算机连接到服务器上。但是,从网络安全性考虑,限制用户登录的时间和在指定的工作站上登录是非常重要的,其基本要求如下。

① 只让用户在其工作期间登录网络。

② 避免用户在存储有重要数据的计算机上登录网络。

(4) 主文件夹设置

主文件夹是存储用户文件和程序的文件夹。它为用户文件提供了一个信息存取位置,这样能方便地对用户文件进行创建、备份、删除、整理等维护工作。一般应为每个用户分配其自己的主文件夹,这样可以避免发生多个用户共用一个文件夹或目录所造成的安全问题。

如果没有为用户分配主文件,系统默认的文件夹是本地计算机的 My Document 文件夹。主文件夹可以存储在网络服务器或用户的本地计算机上。

(5) 配置文件的设置

用户配置文件包含用户所有自行设置的工作环境,如桌面设置、网络连接等。在 Windows Server 2003 中,用户配置文件类型有如下 3 种。

① 本地用户配置文件,该配置文件随计算机的不同而不同。只适合在本地计算机上的环境配置。

② 漫游用户配置文件,该配置文件为用户在网络上登录提供了相同的配置文件,适用于用户在网络任何计算机上的登录。用户可以根据自己的需要更改配置文件。

③ 强制用户配置文件,该配置文件也是一种允许用户配置的文件,但是,用户不能修改配置文件。

(6) 列出用户账户规划表

为了简单明了,同时减少用户账户建立过程中的错误,可以列出用户账户规划表。

2. 设置账户策略

为了增强用户账户密码的安全性和有效性,Windows Server 2003 将账户密码的设置作为安全策略之一提供给管理员。

账户策略设置的对象是系统上的所有账户,而不是针对某一个特别的账户。这些设置是为了让系统能够运行得更安全。如果想要使系统更安全,就要认真地设置这些项目。

设置的方法是使用组策略编辑器中的账户策略设置功能,账户策略包括账户的密码策略、账户的锁定策略和 Kerberos 策略 3 个方面,如图 4.9 所示。

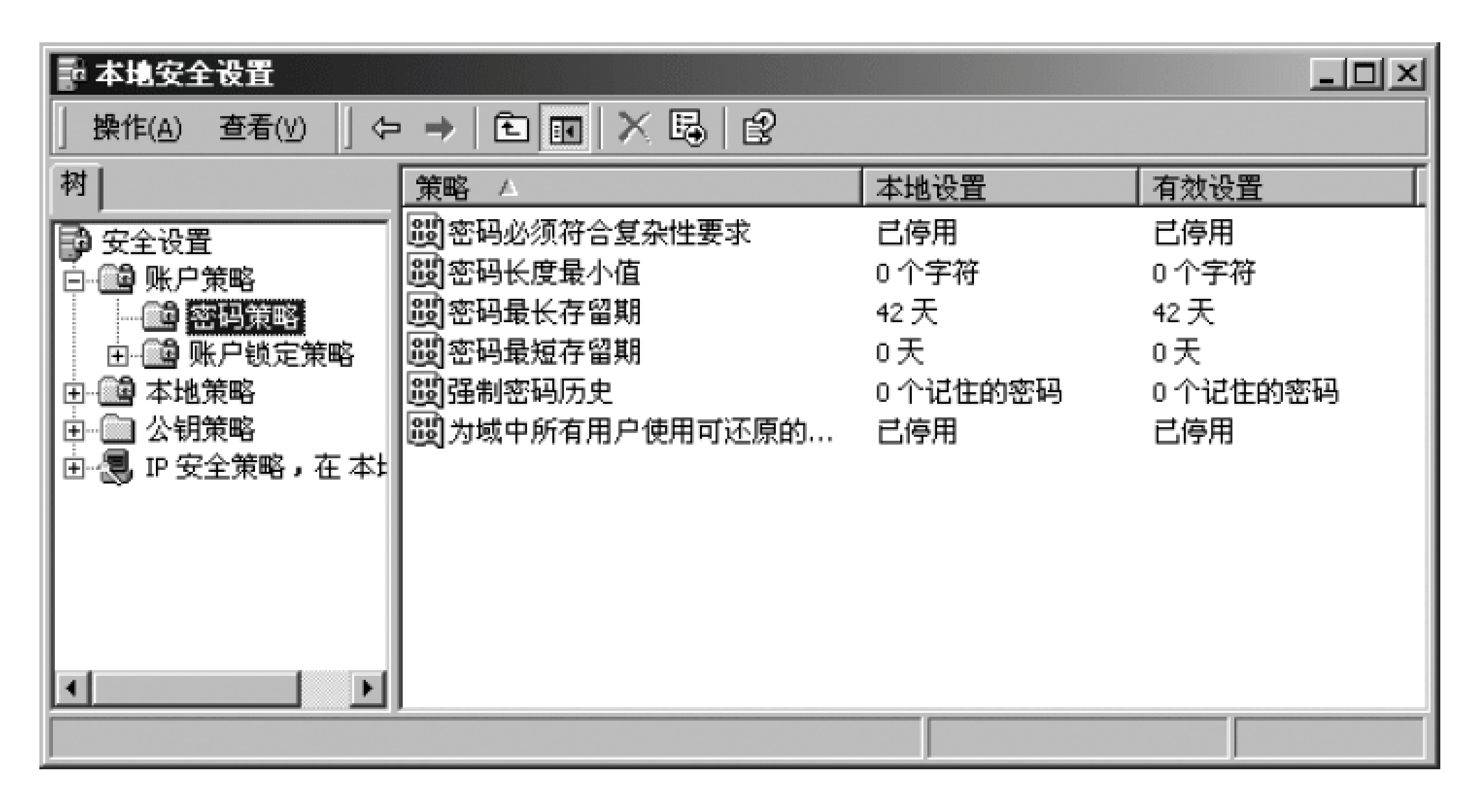


图 4.9 账户策略

(1) 密码策略

密码策略中的设置是有关密码的设置,如图 4.9 所示。密码策略包括下列 6 项限制,如要设置某项,只需要右击对应的行,在快捷菜单中做相应的设置即可。

① 密码最长存留期。用于设置用户密码的有效期限。如果用户在指定的日期内没有更改密码,则在期限到了之后,系统就会强迫用户更改密码,否则就不让用户注册。因为有的用户不愿意改变密码,这样,用户的密码很容易被他人所获取,这无疑造成了系统上的安全漏洞。所以,尽可能不要选择“密码永久有效”这个选项,以免造成系统安全上潜

在的隐患。

② 密码最短存留期。密码最短存留期限制不允许用户频繁更换密码,默认设置 0 表示用户可以任何时候更换密码。

③ 密码长度最小值。可设置用户所使用的密码的最小长度。建议最好限定用户要设置 6 个字符以上的密码,这样,密码就不容易被他人所猜中。

④ 强制密码历史。该项设置的目的是为了避免用户在短时间内重复使用相同的密码,默认情况下系统不会记录密码历史,允许用户不断使用相同的密码。实际上,如果该项设置保留默认值,密码最长存留期也没有什么意义,因为用户可以使用相同的密码替换原来的密码,起不到强制用户更改密码的作用。推荐值迫使用户必须在更换过 3 个不同的密码后才能使用一个过去使用的密码。

⑤ 密码必须符合安装的密码筛选器的复杂性要求。

⑥ 用户必须登录以更改密码。

(2) 账户锁定策略

账户锁定是用来设置用户注册失败时的处理动作。在图 4.10 的账户锁定区中,如果选择了账户不锁定策略的话,系统将对用户的失败注册不做任何处理。为了防止他人猜中用户的密码,建议使用账户锁定策略。



图 4.10 账户锁定策略

锁定账户策略有如下 3 种。

① 账户锁定阀值。设置在用户连续注册失败几次后,锁定其账户。

② 账户锁定时间。设置账户锁定的时间,在锁定指定的时间内,系统禁止打开用户的账户,直到锁定时间结束,系统将自动重新打开用户的账户。

③ 复位账户锁定计数器。这里实际上也是设置时间,如果用户两次注册失败的间隔在该时间范围内,就视为连续注册失败,如果超出该时间范围,则不视为连续失败。

(3) Kerberos 策略

Kerberos 为服务器与客户及服务器与服务器提供了成熟的相互验证身份的方法。

在 Windows Server 2003 中实现的 Kerberos 只负责对用户身份的验证,而不授权访问。在用户的身份得到 Kerberos 确认后,本地安全负责允许或拒绝用户访问资源。

Windows Server 2003 中 Kerberos 策略被定义在域中，Kerberos 策略存放在活动目录里，而且只有 Domain Administrator 组的成员有权改变策略，主要策略如下。

① 强制用户登录限制。用于使每个服务票证请求生效，以确保用户拥有在目标服务器上的登录权限。

② 服务票证最长寿命。票证是客户从服务器收到的一个加密信息。该信息包括有关客户的信息和客户与服务器的会话密钥。客户只有在收到客户会话密钥和来自 Kerberos 代理——密钥分配服务器(KDC)的会话票证后，才能成功地与服务器联系。该设置以分钟为计时单位，不能少于 10 分钟，也不能大于用户票证最长寿命。

③ 用户票证最长寿命。用户票证是 Kerberos 的另一种确认代理的访问者真正身份的票证。从 KDC 返回一个长期密钥，该设置以小时为计时单位，合适的设置为 10 小时。

4.3.3 Windows Server 2003 组管理与策略

建立组的目的是为了设置具有相同工作性质的用户。如某公司的业务部门及会计部门，两个部门都有自己特定的工作任务，因此，可将同一部门或工作性质相同的用户组合在一起工作，构成一个组，便于以后进行权限设置。与创建用户账户类似，可以通过新建或复制创建组。

1. Windows Server 2003 组的形式

从使用领域可将组分为本地组、全局组和通用组 3 种形式。

(1) 本地组

在 Professional 和成员服务器中使用本地组，本地组给用户访问本地计算机上的资源提供权限。

虽然在大多数情况下，单独的用户权利能够直接分配给一个用户，但这是不可取的。因为在用户账户较多的情况下，这会加大管理员的负担及出错的可能性。为了使用户使用本地资源，一般将用户账户添加到本地组。然后给本地组分配资源权限，这样本地组也给用户提供了完成系统任务的权利，如更改计算机上的系统时间，或备份文件和恢复文件。

Windows Server 2003 包含几个内置本地组，这些组带有预先分配的用户权利。例如，内置的 Administrators 组给予成员完成建立用户账户和组账户、备份数据及更改 Windows Server 2003 配置等任务的权利。

内置本地组是预先确定的本地组，它具有预先确定的一组用户权利。用户权利决定用户或内置本地组的成员能够完成的系统任务。Windows Server 2003 的内置本地组包括 Users、Guests、Administrators、Backup Operators、Power Users 和 Operators 6 个组。

(2) 全局组

全局组主要用来组织用户，也就是将多个网络访问权类似的用户账户加入同一个全局组。全局组的特性如下。

① 全局组内的成员只能是域内用户账户或其他全局组。

② 全局组可以访问域内的资源。

(3) 通用组

通用组主要用于指定对多个域中相关资源的访问权限。其成员可以是 Windows Server 2003 中定义的域,并且能被赋予所有域的权限。通用组的特性如下。

① 组内的成员包括任何一个域内的用户账户、通用组、全局组及同一个域内的本地组,但不包括其他域中的本地组。

② 通用组授予所有域的权限,通用组就可以访问任何域中的资源。

2. Windows Server 2003 组的规划

建立组应按照下面准则进行。

① 根据用户的公共需求,逻辑上将用户组织起来。

② 在用户账户驻留的每个域中,为每个用户的逻辑组建立一个全局组,然后将适当的用户账户添加到适当的全局组中。

③ 以资源访问需求为依据建立本地组。

④ 为本地组分配适当的权限。

⑤ 将全局组添加到本地组中。

⑥ 做出组账户的规划表。将组的信息列表,建立组账户规划表,既便于弄清楚组及其关系,又有利于检查和审计组账户的内容。

4.4 NTFS 文件和文件夹的存取控制

存取控制是资源访问安全的基本手段。存取控制就是对用户的访问授权的识别,防止非法访问行为的发生。在 Windows Server 2003 中,存取控制主要通过 NTFS 文件和文件夹(目录)权限设置、共享文件夹权限设置及分布式文件系统对资源的保护等实现。

4.4.1 Windows Server 2003 中的 NTFS 权限

微软为 Windows NT 操作系统设计了一种新的文件系统,这种文件系统就是 NTFS (new technology file system,新技术文件系统),它广泛应用在 Windows NT 操作环境所设计的文件系统,并且广泛应用在 Windows NT 的后续版本 Windows 2003 与 Windows XP 中。与 Windows 系统过去使用的 FAT/FAT 32 格式的文件系统相比,NTFS 具有如下优势。

① 支持长文件名。

② 对文件目录的安全控制。

③ 先进的容错能力。

④ 不易受到病毒和系统崩溃的侵袭。

Windows Server 2003 硬盘内的文件与文件夹如果是位于 NTFS 磁盘分区中,则可以通过"NTFS 权限"来指派用户或组对这些文件与文件夹的使用权限。经过权限指派后,只有具备权限的用户或组才可以访问这些文件与文件夹。

(1) NTFS 文件权限的类型

NTFS 文件权限共有 5 种类型，具体如表 4.1 所示。

表 4.1　NTFS 文件权限的类型

文件权限	说　明
读取	此权限可以读取文件内的数据、查看文件的属性、查看文件的所有者和权限等
写入	此权限可以将文件覆盖、修改文件的属性、查看文件的所有者和权限等。但是，用户即使拥有此权限，也不可以直接更改文件内的数据(如通过 Word 软件来更改)，只能够将该文件整个覆盖掉，因为此权限无法读取文件的属性，除非用户也具备上述“读取”的权限
读取及运行	它除了拥有“读取”的所有权限外，还具有运行应用程序的权限
修改	它除了拥有“写入”与“读取及运行”的所有权限外，还可以更改文件内的数据、删除文件、修改文件名等
完全控制	它拥有所有 NTFS 文件的权限，也就是除了拥有前述的所有权限之外，还拥有“修改权限”与“取得所有权”的权限

(2) NTFS 文件夹权限的类型

Windows Server 2003 中，NTFS 文件夹权限的类型有 6 种，如表 4.2 所示。

表 4.2　NTFS 文件夹权限的类型

文件夹权限	说　明
读取	此权限可以查看该文件夹内文件的名称和文件夹的名称、查看文件夹的属性、查看文件夹的所有者和权限等
写入	此权限可以在文件夹内添加文件与文件夹、修改文件夹的属性、查看文件夹的所有者和权限等
列出文件夹目录	此权限除了拥有“读取”的所有权限之外，还具有“遍历子文件夹”的权限，也就是具备进入子文件夹的功能(即使用户没有权限访问该文件夹，也可以进入此子文件夹)
读取及运行	它拥有与“列出文件夹目录”几乎完全相同的权限，只是在权限的继承方面有所不同，“列出文件夹目录”的权限只由文件夹的功能(即使用户没有权限访问该文件夹，也可以进入此子文件夹)
修改	它除了拥有“写入”与“读取及运行”的所有权限外，还可以删除子文件夹、改变子文件夹的名称等
完全控制	它拥有所有 NTFS 文件夹的权限，也就是除了拥有上述的所有权限外，还拥有“修改权限”与“取得所有权”的权限

4.4.2　在 NTFS 下用户的有效权限

NTFS 权限是指系统管理员或拥有者赋予用户和组访问某个文件和文件夹的权限，通过允许或禁止某些用户或组访问文件夹，实现对资源的保护。NTFS 权限既可以在本地应用，也可以在域中应用。

NTFS 权限分为 NTFS 文件权限和 NTFS 文件夹权限。NTFS 文件权限是应用在

文件上的 NTFS 权限，用来控制用户对文件的访问。NTFS 文件夹权限用来控制用户对文件夹和该文件夹下的文件及子文件夹的访问。默认该文件夹下的文件及文件夹继承该文件夹的 NTFS 权限，因此，通过对文件夹设置权限可以赋予该文件夹下的文件及子文件权限。

除了这几种标准权限外，还有一些特殊的 NTFS 权限，作为这几种标准权限的补充和细化。在特殊 NTFS 权限中把标准权限中的“读取”权限细分为“读取数据”、“读取属性”、“读取扩展属性”和“读取权限”4 种更加具体的权限。

4.4.3 NTFS 权限规则

一个用户可能同时属于多个组，而不同的组对某个文件夹或文件拥有不同的权限，那么该用户对该文件夹或文件具有怎样的权限呢？对于这种多重权限，NTFS 遵循以下规则来分配用户权限的优先级。

1. 权限的累加

用户对某文件夹或文件的有效权限是分配给该用户和该用户所属所有组权限的总和。例如，用户 stu002 同时属于组 stua 和 office02，三者对某文件的权限分别为读取、写入和运行。那么，该用户拥有的有效权限为 3 个权限的总和：读取＋写入＋运行。

2. 文件权限高于文件夹权限

如果某用户拥有对某文件及其所在文件夹不同的权限，则文件的权限高于文件夹的权限。例如，用户 stu002 拥有对文件夹 C:\tools 写入的权限，同时拥有对文件 C:\tools\mylx.txt 读取的权限，那么该用户对文件 C:\tools\mylx.txt 拥有的有效权限为读取权限。

3. 拒绝权限高于其他权限

如果用户对某文件夹或文件同时拥有“拒绝权限”和其他权限时，拒绝权限高于其他权限，即该用户的有效权限为拒绝权限。拒绝权限可以赋予用户，也可以赋予组。例如，用户 stu001 同时属于组 stua 和 stub，三者对某文件的权限分别为读取、写入和拒绝写入。那么，该用户拥有的有效权限为读取权限。虽然组 stua 对该文件拥有写入权限，但组 stub 对该文件拥有拒绝写入权限，拒绝权限高于其他权限，因此，组 stua 赋予的 stu001 写入权限不生效。

4. 权限的继承

默认情况下，新建的子文件夹和文件会继承父文件夹的权限，根目录下的文件或文件夹继承磁盘分区的权限。如果要拒绝继承父文件权限可以通过相关操作实现，如果要强制下级继承也可以通过相关的操作实现。如果一个文件拒绝继承父文件夹权限，然后又设置其父文件夹强制下级继承，那么，该文件被强制继承其父文件夹的权限，即后来设置的权限覆盖前面设置的权限。

5. 复制和移动对权限的影响

对于 NTFS 分区上的文件，从一个文件夹复制或移动到另一个文件夹后，其 NTFS 权限会发生变化。如果 NTFS 分区上的文件或文件夹被复制或移动 FAT 分区中，由于 FAT 分区没有权限设置，原来的权限全部消失。此操作要求操作者必须拥有对目的文件夹的写入权限。

6. A-G-DL-P 规则

A 表示用户贴，G 表示全局组，DL 表示本地域组，P 表示资源权限。A-G-DL-P 规则是将用户账户添加到全局组中，将全局组添加到本地域组中，然后为本地域组分配资源权限。其作用通过如下实例说明。

网络系统中存在两个域 stua 和 teacha，stua 域中的用户 stu001 和 stu002 与 teacha 域中的用户 teach001 和 teach002 都需要访问 teacha 域中的文件夹 data，设置的方法有如下两种。

方法一：在 teacha 中建一个 DL，因为 DL 的成员可以来自所有的域，可分别把域 stua、域 teacha 中的两个用户均加入这个 DL，并把 data 的访问权限赋给 DL。

这样设置虽然可以实现访问权限的要求，但存在如下缺点：DL 存在于 teacha 域中，其管理权也在 teacha 域，如果 stua 域中还有其他人需要访问 data，stua 域管理员是无权做修改的，只能通知 teacha 域管理员，让其对 DL 的成员做修改。如果需要访问的 data 域有 3 个甚至更多，怎么办？全部修改都要由 teacha 域管理员来实现，这种设置太麻烦了。

方法二：在 stua 和 teacha 域都各建一个全局组 Gstu 和 Gteach，stua 域管理员将 stu001 和 stu002 加入 Gstu，teacha 域管理员将 teach001 和 teach002 加入 Gteach，然后在 teacha 域中建立一个 DL，把这两个全局组都加入 teacha 域中的 DL 中，然后把 data 的访问权赋给 DL。

这样，通过组的权限继承，两个全局组都有权限访问文件夹 data 了。由于两个全局组分布在 stua 和 teacha 域中，因此，域管理员可以分别管理自己的全局组。以后有任何修改，都可以自己设置，不用麻烦 teacha 域的管理员了。

4.4.4 NTFS 权限设置

设置 NTFS 权限就是对文件或文件夹设置用户访问的权限，包括设置文件权限、设置文件夹权限、设置 NTFS 特殊权限、设置拒绝继承权、设置强迫继承权等。

1. 设置文件夹的 NTFS 权限

对于指定的文件夹，只有其拥有者、管理员和有完全控制权限的用户才可以设置其 NTFS 权限。下面通过实例说明这样的用户怎样将该文件夹的相关权限赋予其他用户。例如，设置 stua 组的用户 stu001 对文件夹 C:\tools 拥有“写入”权限，详细操作步骤如下。

(1) 以 Administrator 账户登录系统，在 teach.com 域中建立两个用户，如 stu001 和 stu002 及一个组，如 stua，设置这两个账户隶属于 stua 组。在 tools 文件夹上右击，在快捷菜单中选择“tools 属性”命令，在打开的“tools 属性”对话框中选择“安全”选项卡，如图 4.11 所示。

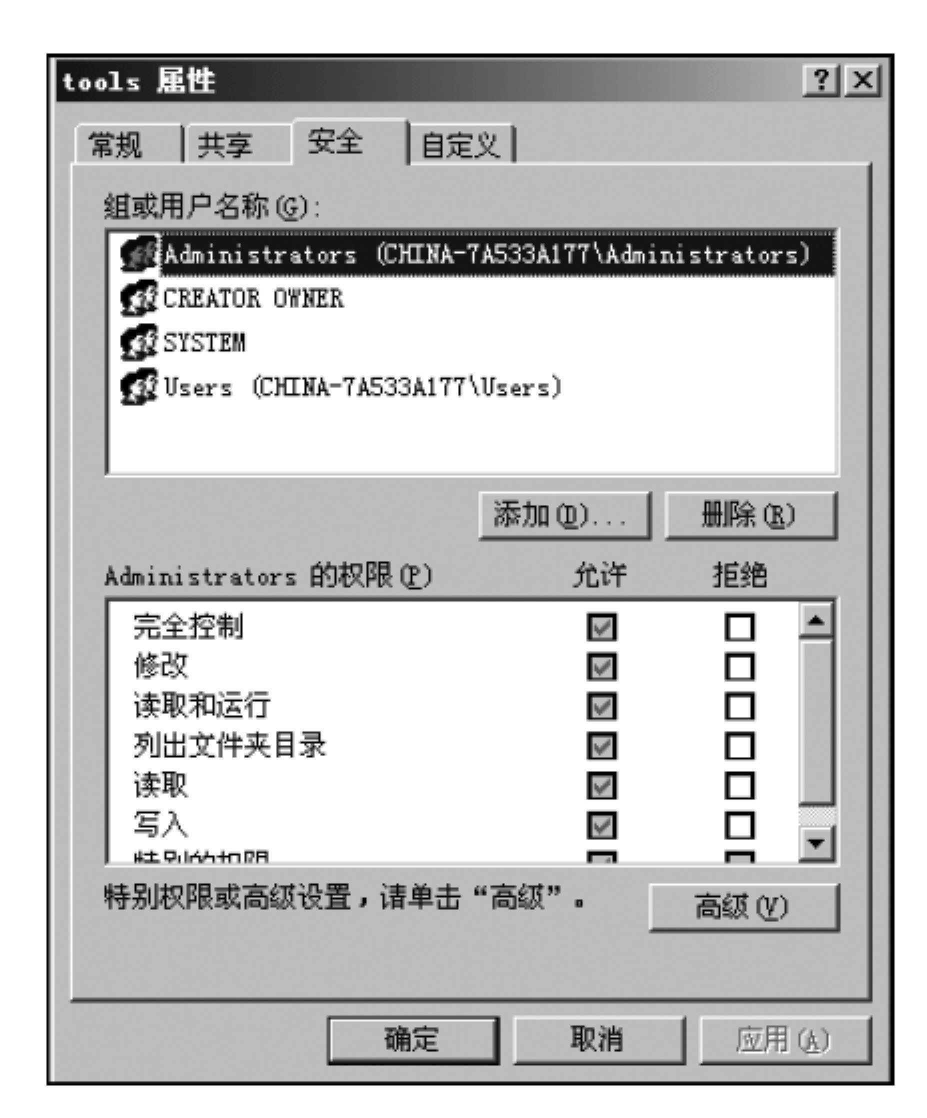


图 4.11 “tools 属性”对话框“安全”选项

(2) 单击“添加”按钮，打开“选择用户或组”对话框，单击“高级”按钮，在打开的对话框中单击“立即查找”按钮，如图 4.12 所示。在搜索结果文本框中找到用户 stu001，选择该用户，如图 4.13 所示，单击“确定”按钮，选择的用户名 stu001 出现在“输入对象名称来选择”列表框中，如图 4.14 所示。



图 4.12 “选择用户或组”对话框

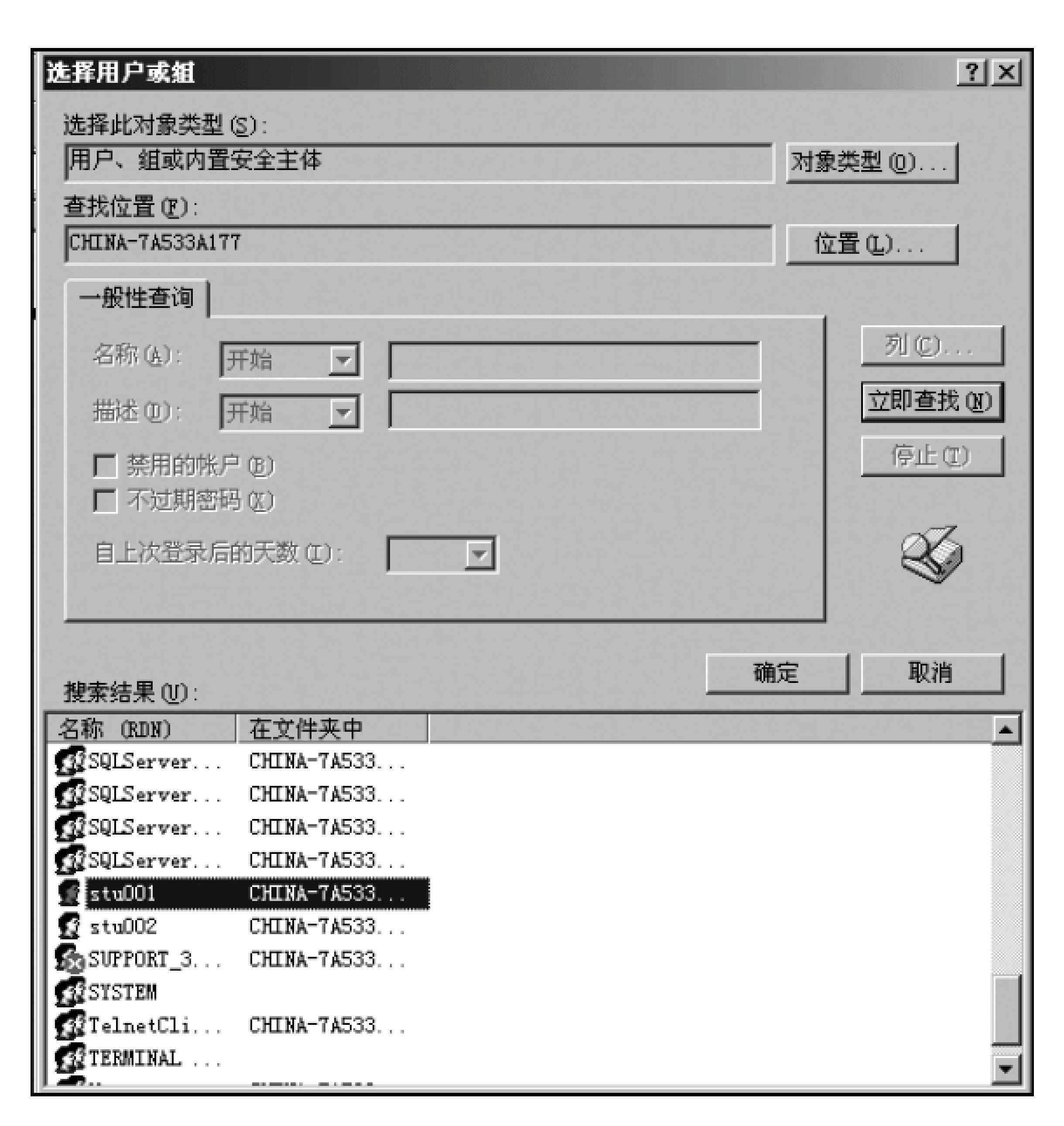


图 4.13 选择用户 stu001



图 4.14 stu001 出现在"输入对象名称来选择"列表框中

(3) 单击"确定"按钮,返回"tools 属性"对话框,在"stu001 的权限"列表框中选中"写入"选项对应的"允许"复选框,如图 4.15 所示,单击"确定"按钮,完成权限的设置。

(4) 注销 Administrator 账户,以 stu001 账户登录系统,在文件夹 C:\tools 中新建文件,验证设置是否成功。在文件夹 C:\tools\remain 中新建文件,验证权限的继承。

2. 设置文件的 NTFS 权限

对于指定的文件,只有其拥有者、管理员和有完全控制权限的用户才可以设置其 NTFS 权限。例如,设置 stua 组的用户 stu002 对 C:\tools\mylx.txt 文件拥有"修改"权限。详细操作如下。

(1) 以 Administrator 账户登录系统。在 mylx.txt 文件上右击,在快捷菜单中选择"属性"命令,在打开的对话框中选择"安全"选项卡,如图 4.16 所示。

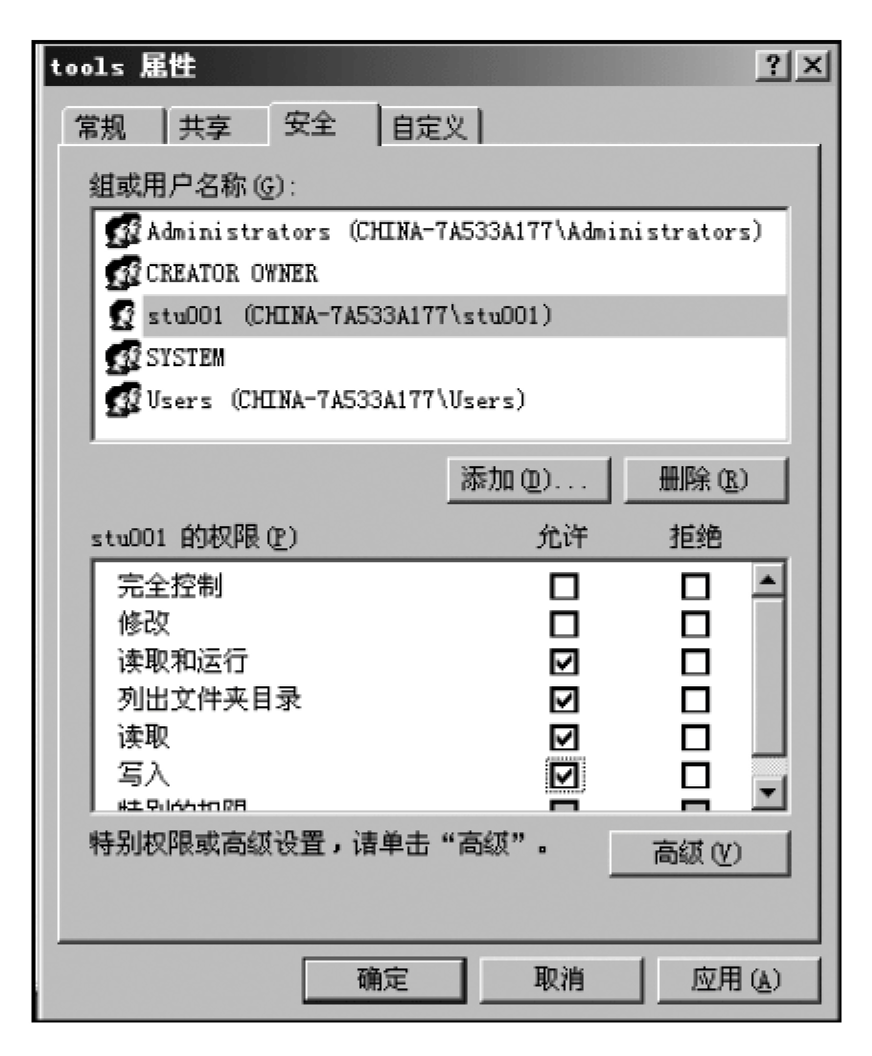


图 4.15 "stu001 的权限"列表框

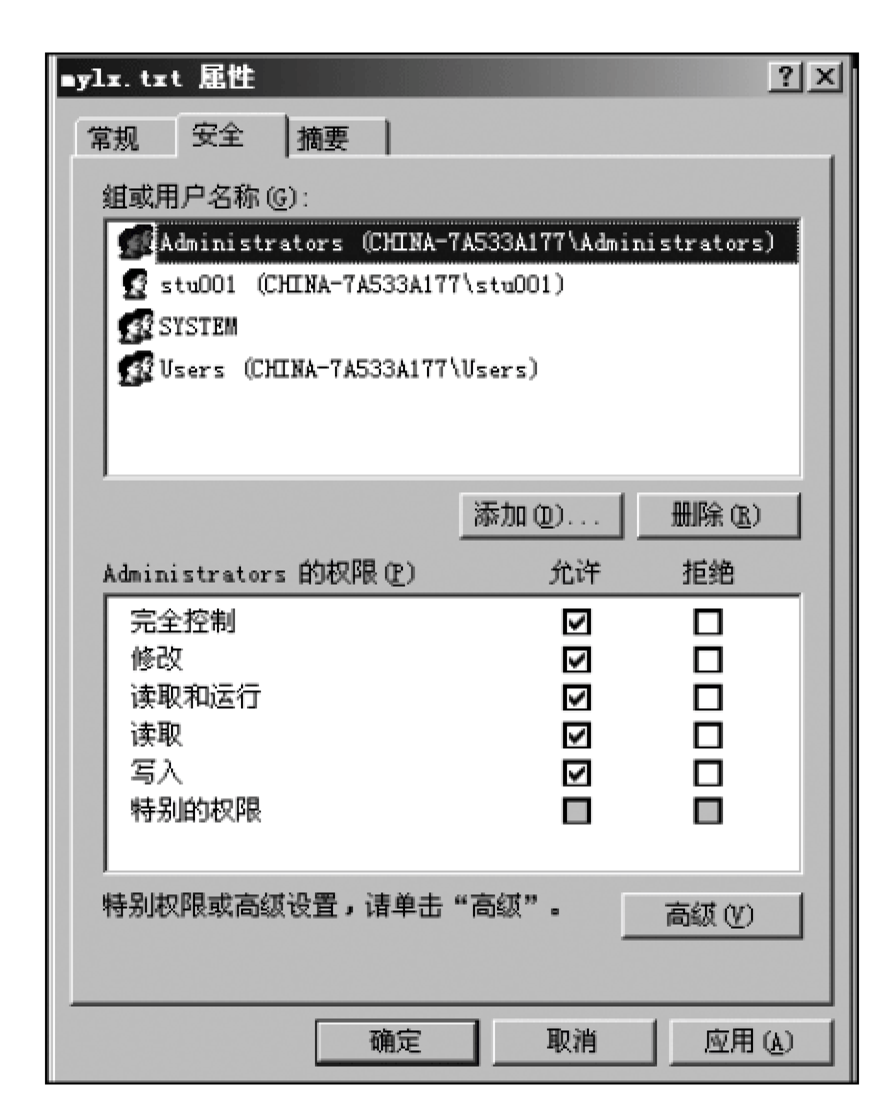


图 4.16 "安全"选项卡

(2) 单击"添加"按钮，打开"选择用户或组"对话框。单击"高级"按钮，在打开的对话框中单击"立即查找"按钮，如图 4.12 所示，在搜索结果文本框中找到用户 stu002，选择该用户。单击"确定"按钮，选择的用户名 stu002 出现在"输入对象名称来选择"列表框中，如图 4.17 所示。



图 4.17 stu002 出现在"输入对象名称来选择"列表框中

(3) 单击"确定"按钮，返回"tools 属性"对话框，在"stu002 的权限"列表框中选中"修改"选项对应的"允许"复选框，如图 4.18 所示，单击"确定"按钮，完成权限的设置。

(4) 注销 Administrator 账户，以 stu002 账户登录系统，对 C:\tools\mylx.txt 文件进行修改并保存，以验证设置是否成功。

3. 设置 NTFS 特殊权限

在特殊权限中有两个较难理解的权限：更改权限和取得所有权。

(1) 更改权限

在标准 NTFS 权限中，只有"完全控制"权限才允许用户拥有更改文件或文件夹的权限，但是，"完全控制"权限同时拥有删除子文件夹或子文件的权限。如果要赋予一个用户

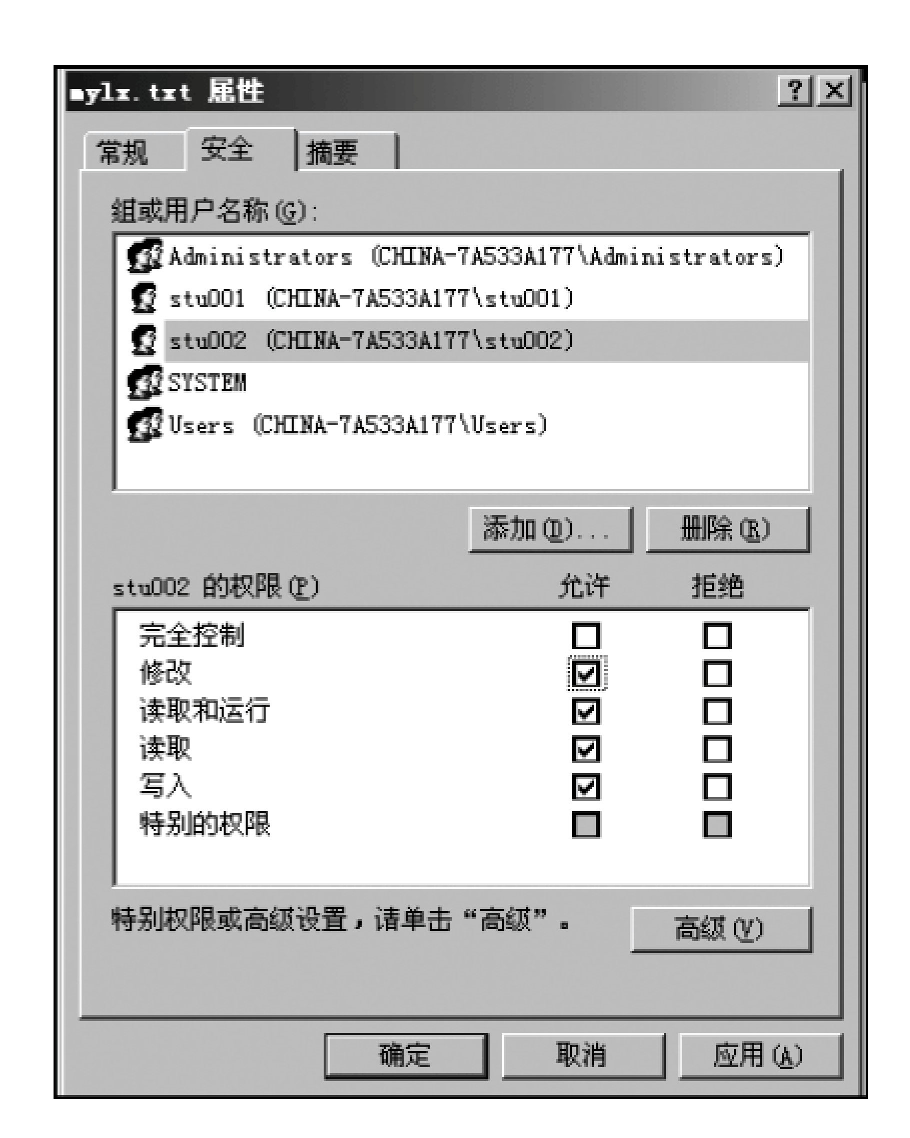


图 4.18 “stu002 的权限”列表框

更改文件或文件夹的权限，又不能让其删除子文件和文件夹，这时就要用到特殊权限中的“更改权限”。例如，设置用户服务 stu002 对文件 C:\tools\mylx.txt 拥有更改权限。

详细的操作步骤是：以 Administrator 账户登录系统。在图 4.18 所示的对话框中单击“高级”按钮，在打开的“mylx.txt 的高级安全设置”对话框的“权限项目”列表框中选择用户 stu002，如图 4.19 所示。然后单击“编辑”按钮，在打开的“mylx.txt 的权限项目”对话框的“权限”列表中选中“更改权限”对应的“允许”复选框，如图 4.20 所示。单击“确定”按钮，返回到上一级对话框，多次单击“确定”按钮，直到关闭全部对话框，完成权限的设置。

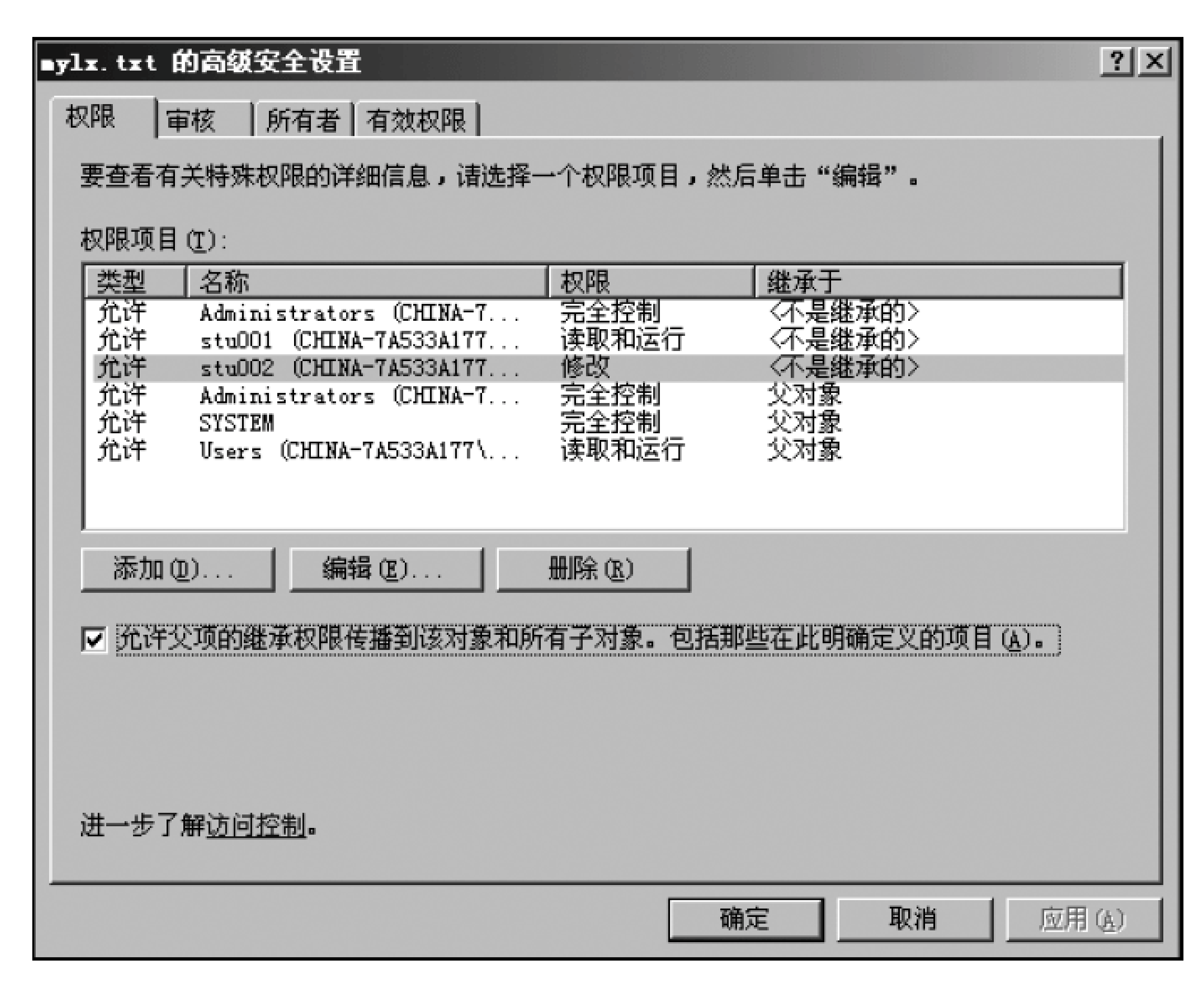


图 4.19 “mylx.txt 的高级安全设置”对话框

(2) 取得所有权

由于各种指派和撤销权限操作可能会造成所有用户(包括管理员)都无法访问某个文件夹或文件的情况。这时就要用到特殊权限中的"取得所有权"。

默认情况下,文件夹或文件的创建者(即所有者)拥有对该文件夹或文件的所有权。取得所有权的用户才能够指派权限。取得所有权有以下两种方式。

文件夹或文件的所有者将"取得所有权"赋予别的用户。

管理员可以取得所有权(但不能转让所有权给别的用户)。

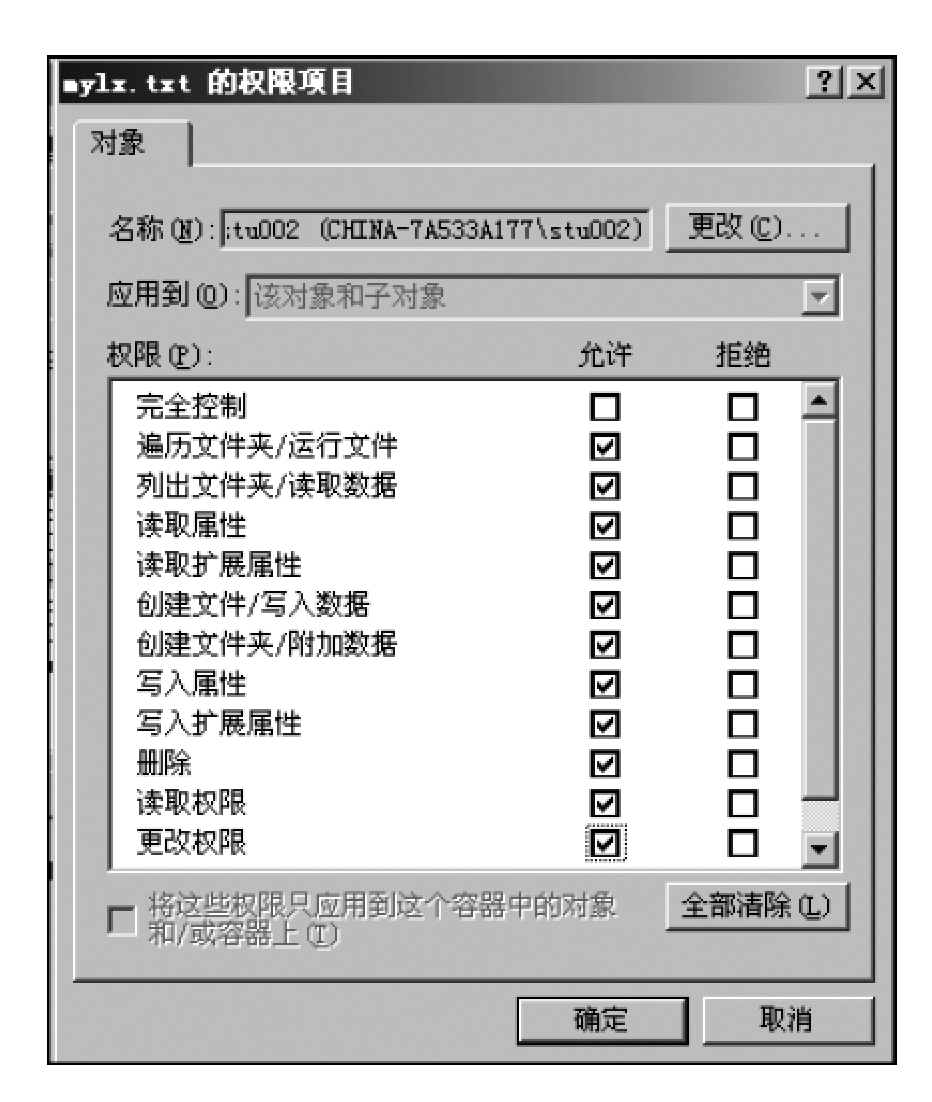


图 4.20 "mylx.txt 的权限项目"对话框

如何让管理员取得所有权呢?以取得由用户 stu001 创建的 C:\tools\stu001_lx.txt 文件所有权为例,详细步骤说明如下。

① 以 Administrator 账户登录系统。在 C:\tools\stu001_lx.txt 上右击,在快捷菜单中选择"属性"命令,在打开的对话框中选择"安全"选项卡。

② 单击"高级"按钮,在打开的"stu001_lx.txt 的高级安全设置"对话框中选择"所有者"选项卡,可以看到"目前该项目的所有者"文本框中显示的所有者为 stu001。在"将所有者更改为"列表框中选择 Administrator,如图 4.21 所示,单击"确定"按钮。返回上一级对话框,单击"确定"按钮,关闭所有对话框,即完成权限设置。



图 4.21 "stu001_lx.txt 的高级安全设置"对话框

③ 重新查看该文件属性，按照上述相同的步骤操作，在打开的“stu001_lx.txt 的高级安全设置”对话框中选择“所有者”选项卡，可以看到“目前该项目的所有者”文本框中显示的所有者为 Administrator。说明 Administrator 成功地取得了该文件的所有权，如图 4.22 所示。



图 4.22　所有权改变后的“stu001_lx.txt 的高级安全设置”对话框

4. 拒绝继承权限和强制继承权限

父文件夹拥有的权限默认被子文件夹及包含在父文件夹中的其他文件继承。当用户修改文件夹的权限时，同时改变了该文件夹包含的子文件夹和文件的权限。



【案例】 利用 AGDLP 规则设置 NTFS 权限

案例分析

某公司的信息处 2 人和销售处 3 人需要对 alldata 文件夹有读取和写入的权限，而其他人员对该文件夹只有读取的权限。

根据公司的要求，设计方案如下。

(1) 在安装 Windows Server 2003 R2 EnterPriseEdition 操作系统的计算机上进行下面的权限设置操作。

(2) 创建 2 个全局组和 1 个本地域组。

(3) 每个全局组中按人员数创建用户账户。

(4) 将 2 个全局组加入本地域组(设名为 loca)。

(5) 为本地域组设置对 alldata 文件夹的读取和写入权限。

(6) 创建其他组织用户账户，设置对 alldata 文件夹的读取权限。

操作步骤

第 1 步 创建全局组(info 和 sale)及相关用户账户,并将相关用户加入各全局组。
第 2 步 创建本地域级(loca),并将全局组(info 和 sale)加入本地域组。
第 3 步 创建其他组(other),并将其他用户加入该组。
第 4 步 为本地域组(loca)设置对 alldata 文件夹的读取和写入权限。
第 5 步 为其他组(other)设置对 alldata 文件夹的读取权限。

4.5 使用审核资源

审核功能用于跟踪用户访问资源的行为与 Windows Server 2003 的活动情况,这些行为或活动称为事件,会被记录到日志文件内,利用“事件查看器”可以查看这些被记录的审核数据。建立审核事件是安全的重要内容之一。通过监控对象的创建和修改可以追踪潜在的安全问题,有助于确保用户账户的可用性,并为指证破坏安全的事件提供依据。

4.5.1 审核事件

在 Windows Server 2003 中,可以被审核并记录在安全日志中的事件类型如下。
(1) 审核策略更改。
(2) 审核登录事件。
(3) 审核对象访问。
(4) 审核过程追踪。
(5) 审核目录服务访问。
(6) 审核特权使用。
(7) 审核系统事件。
(8) 审核账户登录事件。
(9) 审核账户管理。

4.5.2 事件查看器

当 Windows Server 2003 系统有误(如网卡故障)、用户登录/注销的行为或者应用程序发出错误信息等情况时,Windows Server 2003 会将这些事件记录到“事件日志文件”内,可以利用“事件查看器”来检查这些日志,看看到底发生了什么,以便做进一步的处理工作。

Windows Server 2003 的事件日志文件分为以下 4 大类。

(1) 系统日志。Windows Server 2003 会主动将系统产生的错误(如显示故障)、警告(如 CPU 的利用率太高)与系统信息(如某个服务已被启动了)等信息记录到系统日志内。

(2) 安全日志。它会记录“审核策略”所设置的事件发生情况,如某个用户是否曾经读取过某一个文件。

(3) 应用程序日志。它是由应用程序将其所产生的错误、警告或信息等事件记录到此日志文件内。如数据库程序有误时,它可以将此错误记录到应用程序日志内。

(4) 目录服务日志。它会记录由 Active Directory 所发出的诊断或错误信息。这个日志只存在于域控制器内。

1. 查看事件记录

可以通过以下两种方法来启动“事件查看器”。

(1) 右击“我的电脑”,在快捷菜单中选择“管理”→“系统工具”→“事件查看器”命令。

(2) 选择“开始”→“程序”→“管理工具”→“事件查看器”命令。

将出现图 4.23 所示的窗口,可以查看其中的“应用程序”、“安全”、“系统”等日志文件。右边窗格是“系统”日志文件的记录信息,每一行代表一个事件,它提供了以下信息。



图 4.23 事件查看器

① 类型,此事件的类型,如错误、警告、信息等。

② 日期与时间,此事件被记录的日期与时间。

③ 来源,记录此事件的程序名称。

④ 分类,产生此事件的程序可能会将其信息分类,此分类信息会显示在这个“事件”中。

⑤ 事件,每个事件都会被赋予唯一的一个号码,这个号码就是显示在这个“事件”中。

⑥ 用户,当事件发生时,是哪个用户正在使用此计算机,或者此事件是由哪个用户制造出来的。

⑦ 计算机,发生此事件的计算机名称。

若要查看事件的详细信息,可双击该事件或右击该事件,在快捷菜单中选择“属性”命令,打开其属性对话框查看,如图 4.24 所示。

如果要清除某个日志(系统、安全、应用程序等)内的所有事件,则只要右击该日志文件,在快捷菜单中选择“清除所有事件”命令即可。

2. 设置日志文件的大小

可以针对每个日志文件(系统、安全、应用程序等)来更改其设置,例如,日志文件容量的大小等。设置时请选中该日志文件名,右击,在快捷菜单中选择"属性"→"常规"命令,打开图 4.25 所示的对话框。

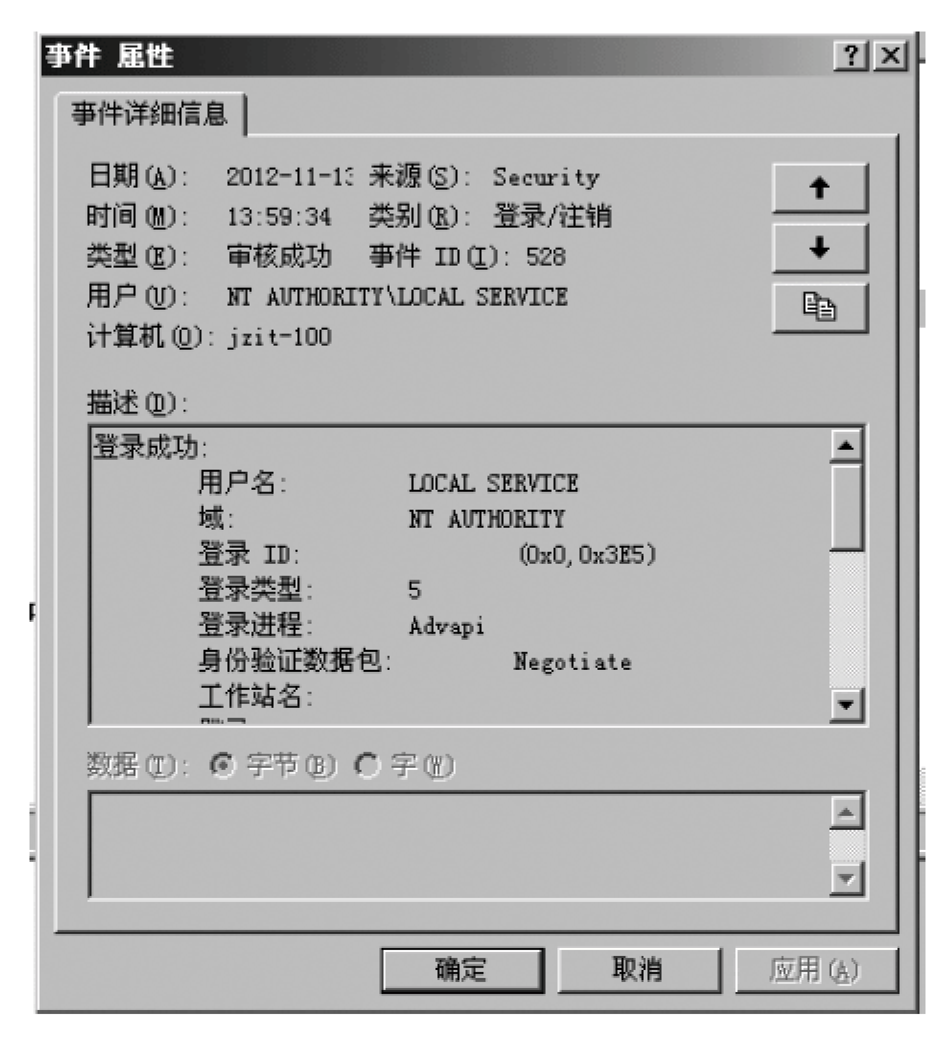


图 4.24 事件的详细信息

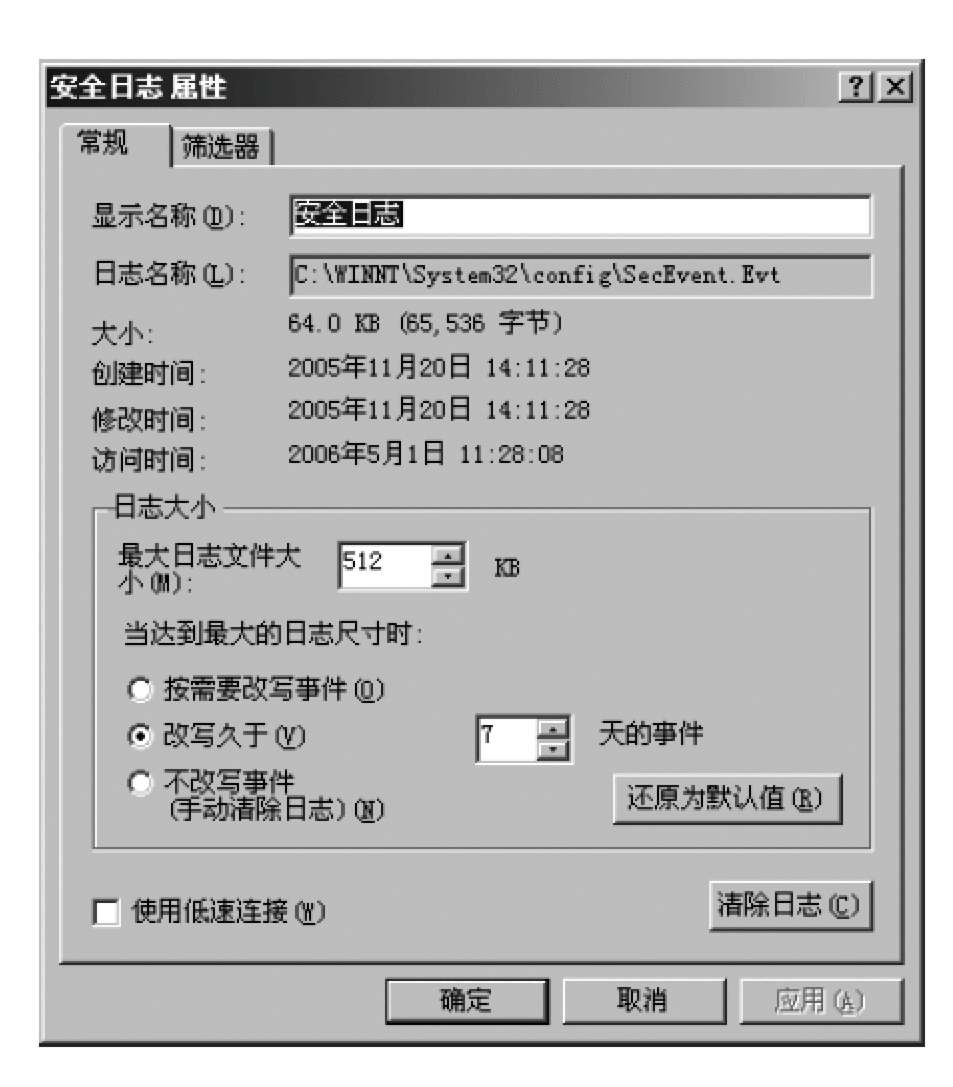


图 4.25 安全日志属性

(1) 最大日志文件大小。用来设置该日志文件的大小,默认为 512KB,可以增加或减少其值,不过日志文件的大小必须是 64KB 的倍数。

(2) 当达到最大的日志尺寸时。即当日志文件满载时,应该如何记录新的事件。

(3) 按需要改写事件。继续记录新的事件,但是会将旧的事件覆盖掉。

(4) 改写久于××天的事件。会将××天前的旧事件覆盖掉,以便继续记录新的事件。

(5) 不改写事件。不会继续记录新的事件,此时必须以手动方式清除日志文件。

(6) 清除日志。将此日志文件清除,如果需要的话,可以在清除之前先将此数据存盘(右击该日志文件,在快捷菜单中选择"另存日志文件"命令保存)。

3. 筛选事件日志中的事件

如果日志文件内的事件太多,造成不易查找事件的情况,可以利用筛选事件的方式让它只显示特定的事件,设置时右击该日志文件,在快捷菜单中选择"属性"→"筛选器"命令,或者右击该日志文件,在快捷菜单中选择"查看"→"筛选"命令实现,出现图 4.26 所示的对话框,从中可以根据事件的类型、事件来源、产生此事件的计算机、事件发生的起始/结束时间等设置选择要显示的事件。

若要取消筛选功能,则可以右击该日志文件,在快捷菜单中选择"查看"→"所有记录"命令实现。

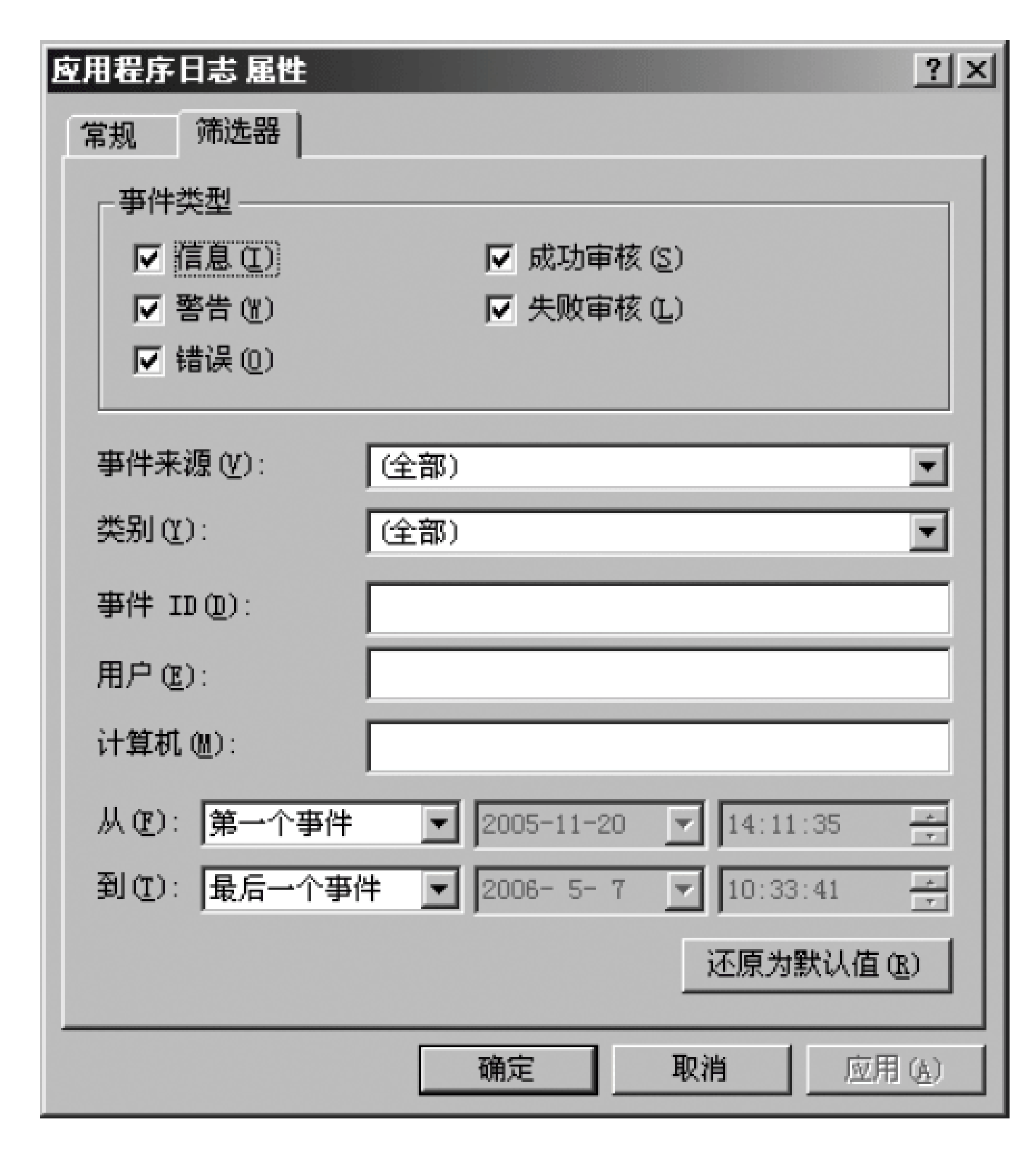


图 4.26 筛选事件日志中的事件

4. 存储日志文件的格式

存储日志文件的格式可以有以下 3 种。

(1) 事件日志。其扩展名为.evt,是"事件查看器"查看的默认日志格式。

(2) 文本(以制表符分隔)。其扩展名为.txt,它是将每一条数据之间利用制表符(Tab)分隔。以此格式存储的文件,可利用一般的文字处理软件(如记事本等)查看,也可供电子表格、数据库等应用程序来读取、导入。

(3) CSV(逗号分隔)。其扩展名为.csv,是将每一条数据之间用逗号分隔。以此格式存储的文件,可利用一般的文字处理软件(如记事本等)来查看,也可供电子表格、数据库等应用程序来读取、导入。

4.5.3 使用审核资源

1. 制定审核策略

审核策略是指是否对系统一些重要事件进行审核。制定事件的审核时需要综合考虑,如果审核太多的事件会造成系统开销太大,审核太少的事件有可能不能保证系统的安全。主要应考虑与系统安全性密切相关的事件。

具体来说,制定审核策略时主要考虑以下问题。

(1) 确定要审核的事件类型

① 访问网络资源,如文件、文件夹或打印机等。

② 用户登录和注销。

③ 关闭和重新启动运行 Windows Server 2003 的计算机。

④ 修改用户账户和组。

（2）确定审核成功的事件与审核失败的事件或者两者都审核

① 账户管理：成功、失败。

② 登录事件：成功、失败。

③ 对象访问：失败。

④ 策略更改：成功、失败。

⑤ 特权使用：失败。

⑥ 系统事件：成功、失败。

⑦ 目录服务访问：失败。

⑧ 账户登录事件：成功、失败。

（3）确定查看安全日志的时间表

要审核用户访问资源的情况，必须经过以下两个步骤。

① 设置审核策略。条件是只有具备 Administrator 权限的用户才能设置审核策略。

② 设置要审核的资源。必须具备“管理审核及安全日志”权限的用户才可以审核资源的使用情况，默认是只有 Administrators 组内的成员才有此权限。可以利用组策略内的“用户权利指派”策略给予其他用户这个权限。如果要审核文件或文件夹的使用情况，则这些文件与文件夹必须位于 NTFS 磁盘分区内，FAT16/FAT32 并不支持审核的功能。另外，最好将事件日志归档，以便于以后查询。

按照审核策略所记录的数据记录在“安全日志”内，利用“事件查看器”查看此日志。

2. 审核策略的设置

审核策略的设置是通过“组策略”或“本地安全策略”进行的。根据目前正在使用的计算机与设置的对象决定使用“组策略”或“本地安全策略”。

另外，如果在本地计算机、站点、域与组织单位内都分别设置了审核策略，则这些审核策略的应用顺序如下。

（1）本地审核策略（通过“本地安全策略”设置）。

（2）站点的审核策略。

（3）域的审核策略。

（4）组织单位（OU）的审核策略。

审核策略应用的总原则是：应用顺序在后的审核策略会覆盖应用顺序在前的审核策略，例如，若在域的审核策略与本地审核策略的设置有冲突时，则以应用顺序在后的域审核策略内的设置为其最终设置。



【案例】 在 Windows Server 2003 中审核启动和登录事件

案例分析

在 Windows Server 2003 中，我们可以对事件进行审核，从而发现一些不正常的安全行为。

操作环境

(1) 一台连上 Internet 的计算机。

(2) Windows Server 2003 系统。

操作步骤

第 1 步 登录并配置安全审核。

(1) 以 Administrator 的身份登录。

(2) 打开嵌入式管理单元本地安全策略。

(3) 到“本地策略”→“安全审核”中，并且对下面每一个内容进行配置。

① 账户登录事件审核：成功，失败。

② 账户管理审核：成功，失败。

③ 登录事件审核：成功，失败。

④ 策略更改审核：成功，失败。

⑤ 特权使用审核：失败。

⑥ 系统事件审核：失败。

(4) 从系统中注销。

第 2 步 审核登录事件。

(1) 以 Administrator 身份重复几次失败登录。

(2) 以 Administrator 身份登录进入系统。

(3) 打开事件查看器。

(4) 在事件查看器中，查看安全日志窗口。

(5) 搜寻记录失败登录企图的正确数字(如果需要指导，可以查看前面的审核项列表)。

(6) 注销，随后以 Administrator 注册进入系统，并查看事件查看器。

(7) 清除安全和系统日志。

第 3 步 审核启动事件。

(1) 重新启动 Windows Server 2003 并以 Administrator 身份重新登录。

(2) 打开事件查看器并查看系统日志。

(3) 按下机器上的电源按钮并保持 5 秒钟以上，Windows Server 2003 将会突然关闭。

(4) 打开事件查看器并找到 6008 号事件。

4.6 Windows Server 2003 的安全与安全设置

Windows Server 2003 是微软公司在 Windows 2000 系列的基础上改进推出的，它集成了功能强大的应用程序环境，具有更广泛的适应性和更便捷的管理。

对于网络系统管理员来说，最关心的事情莫过于系统的安全。Windows Server 2003

作为微软公司最新推出的服务器操作系统，与 Windows 2000/XP 系统相比，各方面的功能确实得到了增强，尤其在安全性方面。但任何事物都不是十全十美的，Windows Server 2003 也存在系统漏洞和安全隐患。无论用计算机欣赏音乐、上网冲浪、运行游戏，还是编写文档都不可能避免地受到新病毒和恶意软件的威胁，如何让 Windows Server 2003 更加安全，就成为广大用户十分关注的问题。

4.6.1 Windows Server 2003 的安全

Windows Server 2003 系统不仅继承了 Windows 2000/XP 的易用和稳定的特点，还提供了更高的硬件支持和更强大的安全功能，无疑是中小型网络应用服务器的首选。Windows Server 2003 系统提供的提高密码的破解难度、启用账户锁定策略、限制用户登录、限制外部连接、系统审核机制、监视开放端口和连接、监视进程和系统信息等安全策略，可确保网络安全和服务器的正常运行。

1. 提高密码的破解难度

在 Windows Server 2003 中，可以通过在安全策略中设定“密码策略”来提高密码的破解难度。Windows Server 2003 系统的安全策略可以根据网络的情况，针对不同的场合和范围进行有针对性的设定。例如，可以针对本地计算机、域及相应的组织单元进行设定，这将取决于该策略要影响的范围。以域安全策略为例，其作用范围是网中所指定域的所有成员。在域管理工具中运行“域安全策略”工具，就可以针对密码策略进行相应的设定。密码策略也可以在指定的计算机上用“本地安全策略”来设定，同时也可在网络中特定的组织单元通过组策略来设定。

2. 启用账户锁定策略

Windows Server 2003 系统的账户锁定是指在某些情况下（如账户受到采用密码词典或暴力猜解方式的攻击），为保护该账户的安全而将其进行锁定，使其在一定的时间内不能再次使用。默认情况下并没有设定这种锁定策略，用户可根据情况自行设置账户锁定。一般设定如果 3 次登录全部失败，系统就会锁定该账户。一旦该账户被锁定后，既使合法用户也无法使用了，只有系统管理员才能重新启用该项账户。为方便用户，可以同时设定锁定的时间，这样从开始锁定账户时进行计时，当锁定时间超过该时间后自动解锁。虽然该项设置会给用户造成一些不便，但它可以有效地避免自动猜解工具的攻击。“步”是指定账户锁定的阈值，即确定该账户无效登录的次数。一般设定该数值为 3。

3. 限制用户登录

用户还可以通过对登录行为进行限制来保障其账户的安全。这样即使密码被泄露，系统也可以在一定程度上阻止黑客的入侵。Windows Server 2003 网络用户可运行“Active Directory 用户和计算机”管理工具，选择相应的用户并设置其“账户属性”。在“账户属性”设置中可对其登录时间和地点进行限制。另外，还可以通过“账户”选项限制登录时的行为，如使用“用户必须用智能卡登录”就可避免直接使用密码验证。此外，还可

以引入指纹验证等更严格的手段。

4. 限制外部连接

对于企业网络来说，通常需要为一些远程拨号用户(业务人员或客户)提供拨号接入服务。远程拨号访问技术实际上是通过低速拨号连接将远程计算机接入企业内部网。由于该连接无法隐藏，因此，常常成为黑客入侵企业内部网的最佳入口，但采取一定的措施可以有效地降低此风险。基于 Windows Server 2003 的远程访问服务器，默认情况下将允许具有拨入权限的所有用户建立连接，因此，如果合理地设置用户账户的拨入权限，严格限制拨入权限的分配范围，即可较好地限制外部连接。在 Windows Server 2003 系统中，如果活动目录工作在 Native-mode(本机模式)下，就可以通过存储在访问服务器上或 Internet 验证服务器上的远程访问策略来进行管理。

5. 限制特权组成员

Windows Server 2003 系统还有一种非常有效的防范黑客入侵和管理疏忽的辅助手段，这就是“受限制的组”安全策略。该策略可保证组成员是固定的。在域安全策略的管理工具中添加要限制的组，在“组”对话框中输入或查找要添加的组，然后配置该受限制的组成员，当安全策略生效后，可防止黑客将后门账户添加到该组中。

6. 启用系统审核机制

系统审核机制可以对系统中的各类事件进行跟踪记录并写入日志文件，以供管理员分析、查找系统和应用程序故障及各类安全事件，对 Windows Server 2003 系统的服务器和工作站系统来说，为了不影响系统的性能，默认的安全策略并不对安全事件进行审核。从“安全配置和分析”工具用 SecEdit 安全模板进行的分析结果可见，这些有特殊标记的审核策略应该已经启用，这可用来发现来自外部和内部的黑客的入侵行为。对于关键的应用服务器和文件服务器来说，应同时启用共同的安全策略。如果已经启用了“审核对象访问”策略，那么就要求必须使用 NTFS 文件系统。NTFS 文件系统不仅提供对用户的访问控制，还可以对用户的访问操作进行审核。但这种审核功能需要针对具体的对象来进行相应的配置。

在被审核对象“安全”属性的“高级”属性中添加要审核的用户和组，选择要审核的用户后，就可以设置对其进行审核的事件和结果。在所有的审核策略生效后，就可以通过检查系统的日志来发现黑客的蛛丝马迹。

7. 监视开放的端口和连接

在系统中启用安全审核策略后，系统管理员应经常看安全日志记录，否则就失去了及时补救和防御的时机。对日志的监视只能发现已经发生的入侵事件，对正进行的入侵和破坏行为却无能为力。这时，就需要系统管理员来掌握一些基本的实时监视技术。

黑客或病毒入侵系统后通常会在系统中留下后门，同时会与外界建立一个 Socket 会话连接进行通信，这时利用 netstat 命令进行会话状态的检查就可能发现它，在这里就可

以查看已经打开的端口和已经建立的连接。当然可以采用一些专用的检测程序对端口和连接进行检测。

8. 监视共享

黑客通过共享入侵系统是很方便的，最简单的就是利用系统隐含的管理共享。因此，只要黑客能扫描到用户的IP和密码，就可使用netuse命令连接到共享上，另外，当发现含有恶意脚本的网页时，此时计算机硬盘也就可能被共享，因此，监测本机的共享连接是非常重要的。监测本机共享连接的具体方法为：在Windows Server 2003系统中，打开“计算机管理”工具，并展开“共享文件夹”选项，选择其中的“共享”选项就可以查看其右面窗口，以检查是否有新的可疑共享。如果有可疑共享，就应该立即删除。另外，还可以通过选择“会话”选项，来查看连接到计算机上所有共享的会话。

9. 监视进程和系统信息

对于木马和远程监控程序，除了监视开放的端口外，还应通过任务管理器的进程查看功能来查看进程，在安装Windows Server 2003系统支持工具后就可以获得一个进程查看工具Process Viewer。隐藏的进程通常寄宿在其他进程下，因此，查看进程的内存映像也许能发现异常。有些木马会把自己注册成一个服务，从而可避免在进程列表中现形，因此，人们还应该加强对系统中其他信息的监视，对系统信息中的软件环境下的各项内容进行相应的检查。

4.6.2 Windows Server 2003的安全设置

下面介绍一些Windows Server 2003系统常用的安全操作和设置。

1. 清除默认共享隐患

使用Windows Server 2003系统在默认安装时，会产生默认的共享文件夹。虽然用户并没有设置共享，但每个盘符都被Windows自动设置了共享，其共享名为盘符后面加一个符号$（共享名为c$、d$、ipc$等），这样一来，只要攻击者知道了该系统的管理员密码，就有可能通过输入“\\工作站\点共享名\共享名称”来打开系统的指定文件夹，用户精心设置的安全防范就不安全了。因此，应将Windows Server 2003系统默认的共享隐患从系统中清除。具体可采用以下步骤。

（1）选择“开始”→“运行”命令，在出现的对话框中输入“gpedit.msc”，确认后即可打开组策略编辑器。

（2）选择“用户配置”→“Windows设置”→“脚本（登录/注销）”→“登录”命令，如图4.27所示。

（3）双击“登录”图标，在出现的“登录 属性”对话框中单击“添加”按钮。

（4）在出现的“添加脚本”对话框的“脚本名”文本框中输入delshare.bat，单击“确定”按钮即可，如图4.28所示。

（5）重新启动计算机。



图 4.27 组策略编辑器

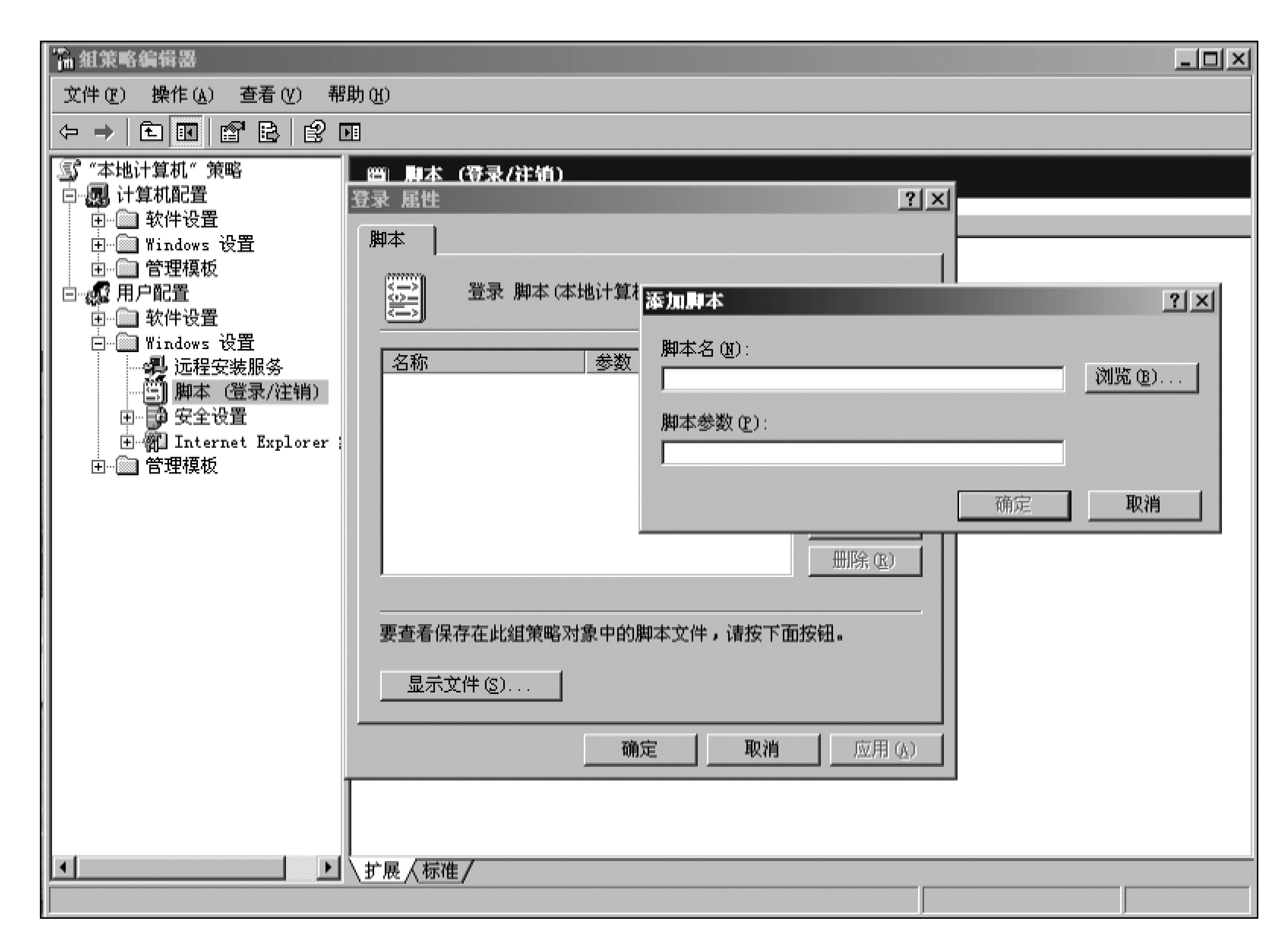


图 4.28 清除默认共享

这样就可以自动将系统所有的隐藏共享文件夹全部取消，从而将系统安全隐患降到最低限度。

2. 禁止非法访问应用程序

Windows Server 2003 是一种服务器操作系统。为了防止非法用户登录到系统中并

随意启动服务器中的应用程序，给服务器的正常运行带来不必要的麻烦，可根据不同用户的访问权限来限制其调用应用程序的操作。实际上，我们只要使用组策略编辑器作进一步的设置，即可实现这一目的，具体步骤如下。

（1）打开“组策略编辑器”窗口，然后选择“‘本地计算机’策略”→“用户配置”→“管理模板”→“系统”选项，如图 4.29 所示。



图 4.29 组策略编辑器中的系统设置

（2）双击“只运行许可的 Windows 应用程序”，在“设置”中选择“已启用”。

（3）单击“允许的应用程序列表”旁的“显示”按钮，弹出“显示内容”对话框。

（4）单击“添加”按钮来添加允许运行的应用程序，如图 4.30 所示。

这样操作后一般用户只能运行“允许的应用程序列表”中列出的程序。

3. 禁用 IPC 连接

IPC＄(Internet process connection)是共享“命名管道”的资源，它是为了使进程间通信而开放的命名管理。通过提供可信任的用户名和口令，连接双方计算机即可建立安全的通道，并以此通道进行加密数据的交换，从而实现对远程计算机的访问。它是 Windows NT/2000/Server 2003 特有的功能。但它有一个特点，即在同一时间内，两个 IP 之间只允许建立一个连接。系统在提供了 IPC＄功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑共享(c＄、d＄、e＄等)和系统目录 windows(admin＄)共享。这虽然为系统管理员的管理提供方便，但也为 IPC 入侵者提供了方便条件，导致系统的安全性能降低，因此，为了安全起见，应禁用 IPC 连接。可以通过修改注册表来实现禁用 IPC 连接。

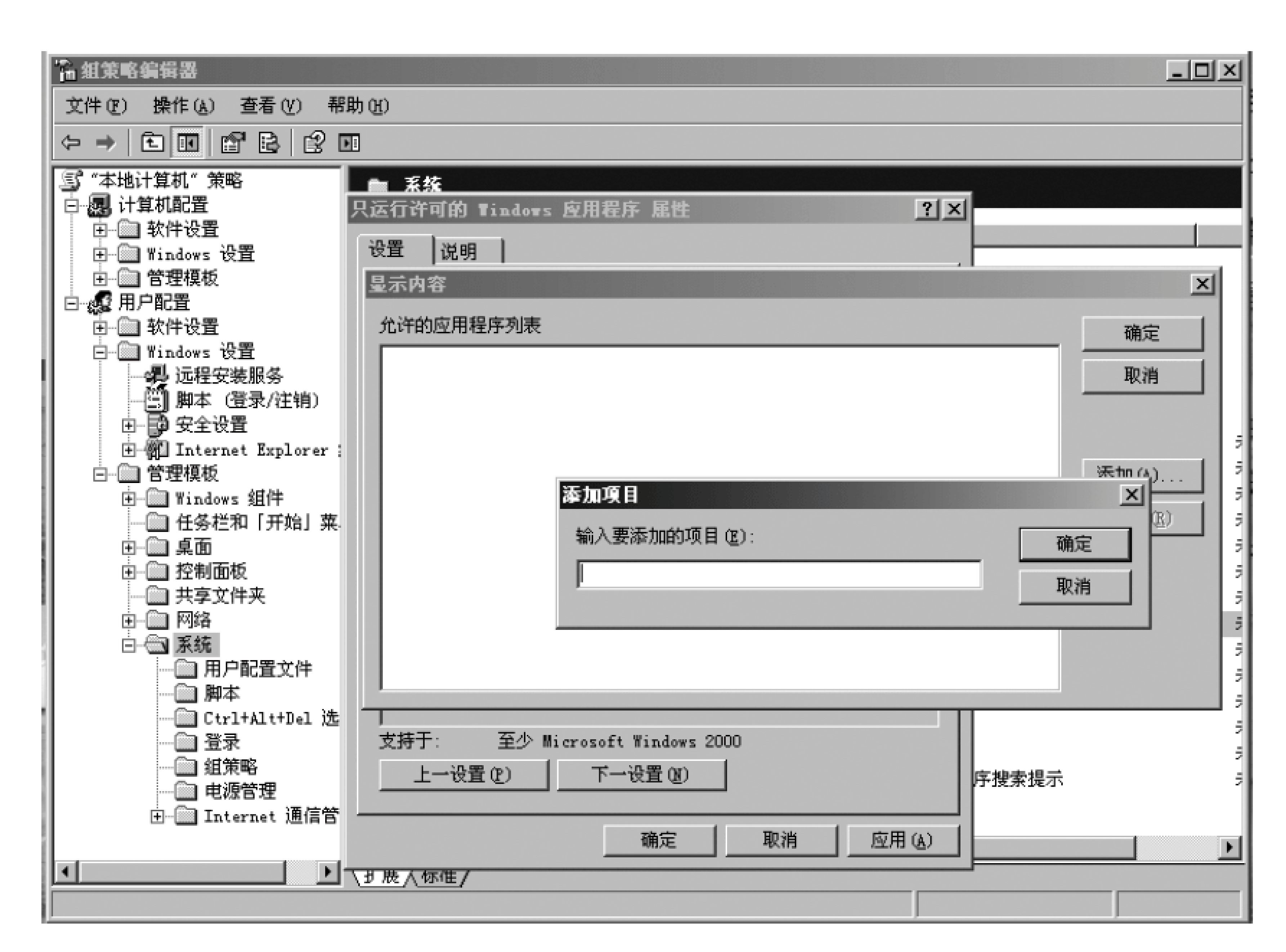


图 4.30 “添加项目”对话框

4. 清空远程可访问的注册表路径

Windows Server 2003 系统提供了注册表的远程访问功能,只有将远程可访问的注册表路径设置为空,才能有效地防止黑客利用扫描通过远程注册表读取计算机的系统信息。设置远程可访问注册表路径为空的步骤如下。

(1) 打开组策略编辑器,展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”选项。

(2) 单击“安全选项”,双击右侧窗口中的“网络访问:可远程访问的注册表路径”选项。

(3) 在打开的“网络访问:可远程访问的注册表路径 属性”窗口中,将可远程访问的注册表路径和子路径内容全部设置为空,再单击“确定”按钮即可。

另外,在进行安全设置时,对图 4.31 所示的本地策略的安全选项设置可以考虑将“网络访问:可匿名访问的共享”、“网络访问:可匿名访问的命名管道”和“网络访问:可远程访问的注册表路径和子路径”三项全部删除;将“不允许 SAM 账户的匿名枚举”、“不允许 SAM 账户和共享的匿名枚举”、“网络访问:不允许存储网络身份验证的凭据或.NETPassports”和“网络访问:限制匿名访问命名管道和共享”四项更改为“已启用”。

5. 关闭不必要的端口和服务

对于个人用户来说,系统安装过程中默认的有些端口没有什么用,应该关掉这些端口,即关闭无用的服务。

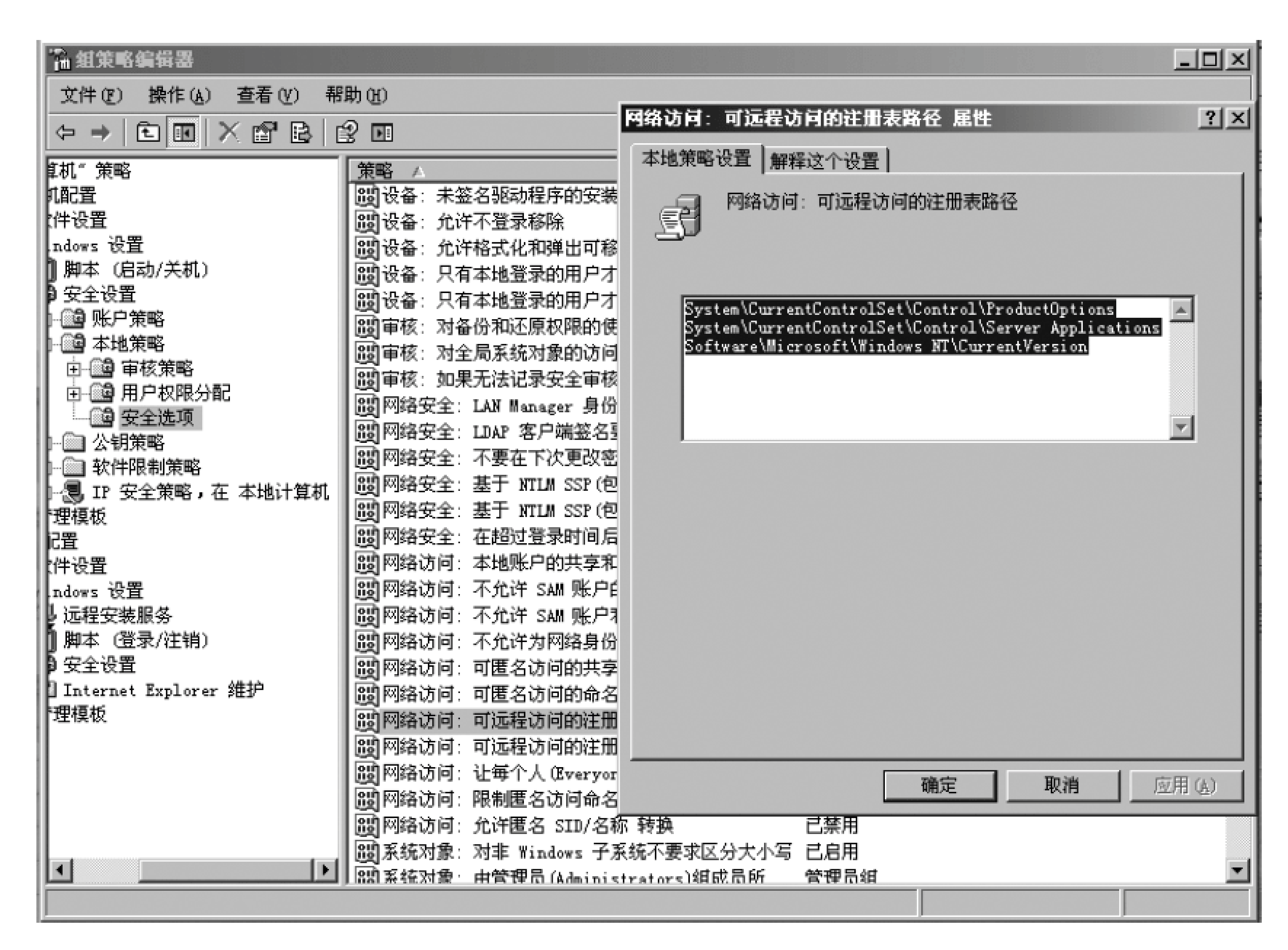


图 4.31 进入远程可访问的注册表路径

(1) 关闭 139 端口

139 端口是 NetBIOS 协议所使用的会话服务端口，在安装了 TCP/IP 协议的同时，NetBIOS 也会被作为默认设置安装到系统中。该端口的开放意味着硬盘可能会在网络中共享，网上黑客可通过 NetBIOS 了解用户计算机中的一切。在以前的 Windows 版本中，只要不安装微软网络的文件和打印共享协议，就可关闭 139 端口。但在 Windows Server 2003 系统中，要单独进行关闭 139 端口的操作才行。关闭 139 端口的具体步骤如下。

① 右击“网络邻居”，在快捷菜单中选择“属性”命令，进入“网络和拨号连接”。

② 右击“本地连接”，在快捷菜单中选择“属性”命令，打开“本地连接属性”页面。

③ 取消选中“Microsoft 网络的文件和打印共享”复选框，如图 4.32 所示。

④ 选中“Internet 协议(TCP/IP)”复选框，依次单击“属性”→“高级”→“WINS”，选中“禁用 TCP/IP 上的 NetBIOS ”单选按钮，即可完成任务，如图 4.33 所示。

(2) 关闭 445 端口

445 端口是一把“双刃剑”，有了它用户可以在局域网中轻松访问各种共享文件夹或共享打印机，但也正是因为有了它，黑客们才有了可乘之机。他们可通过该端口偷偷共享用户的硬盘，甚至会在悄无声息中将用户的硬盘格式化。用户要做的就是想办法不让黑客有机可乘，封堵住 445 端口的漏洞，办法是：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters
```

右击 Parameters 选项，在快捷菜单中选择“新建”→“DWORD 值”命令，将 DWORD 值命名为 SMBDeviceEnabled，数值为 0。

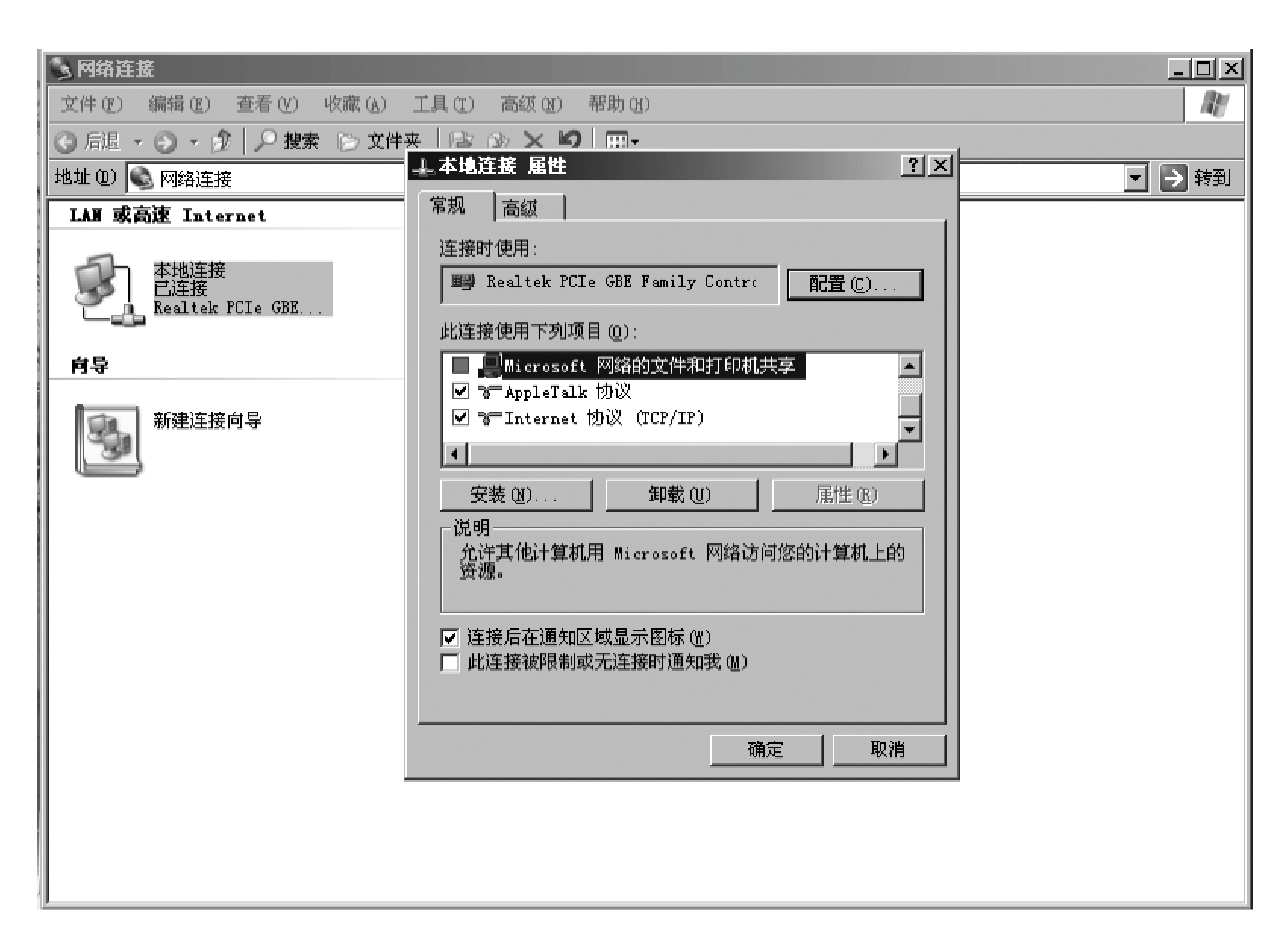


图 4.32 网络的文件和打印共享

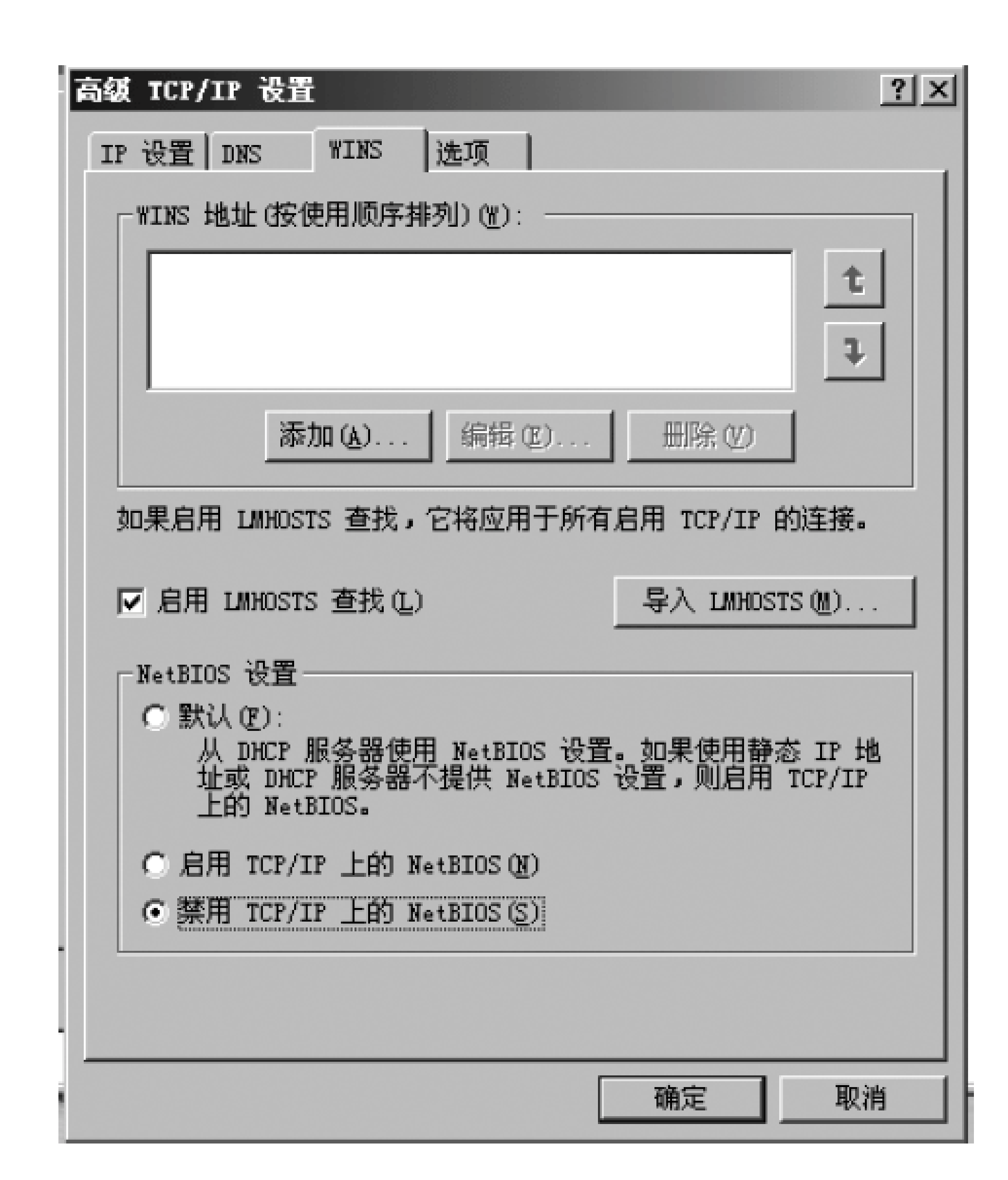


图 4.33 禁用 TCP/IP 上的 NetBIOS

(3) 关闭 135 端口

关闭 135 端口的步骤如下。

① 选择"开始"→"运行"命令,在出现的对话框中输入 dcomcnfg,单击"确定"按钮,打开组件服务。

② 在"组件服务"窗口选择"计算机"选项,如图 4.34 所示。在"计算机"选项中,右击"我的电脑",在出现的对话框中选择"属性"命令。

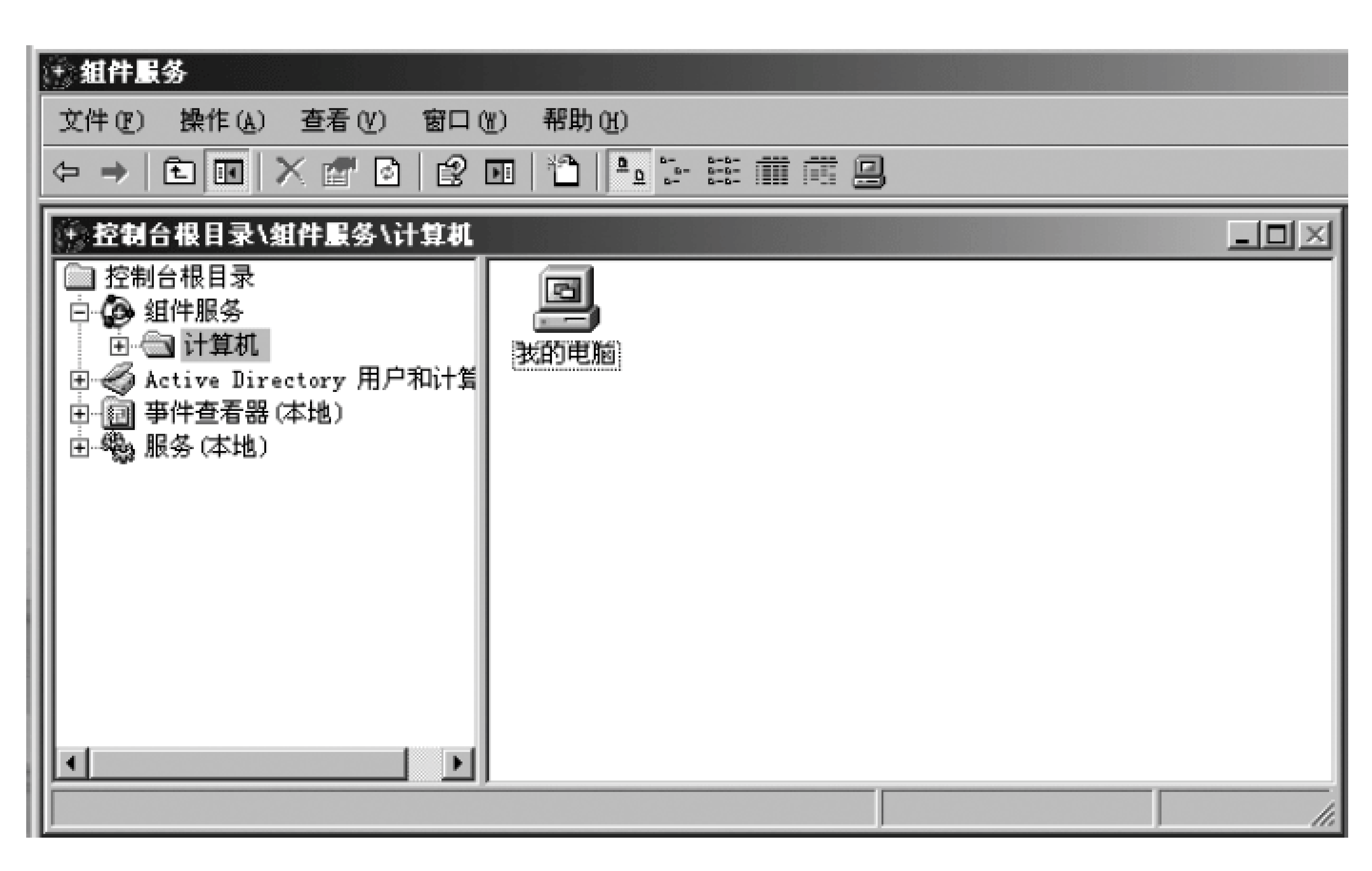


图 4.34 组件服务

③ 在出现的"我的电脑 属性"对话框的"默认属性"选项卡中，取消选中"在此计算机上启用分布式 COM"复选框，如图 4.35 所示。

④ 选择"默认协议"选项卡，选中"面向连接的 TCP/IP"选项，单击"移除"按钮。

⑤ 单击"确定"按钮，设置完成，如图 4.36 所示。

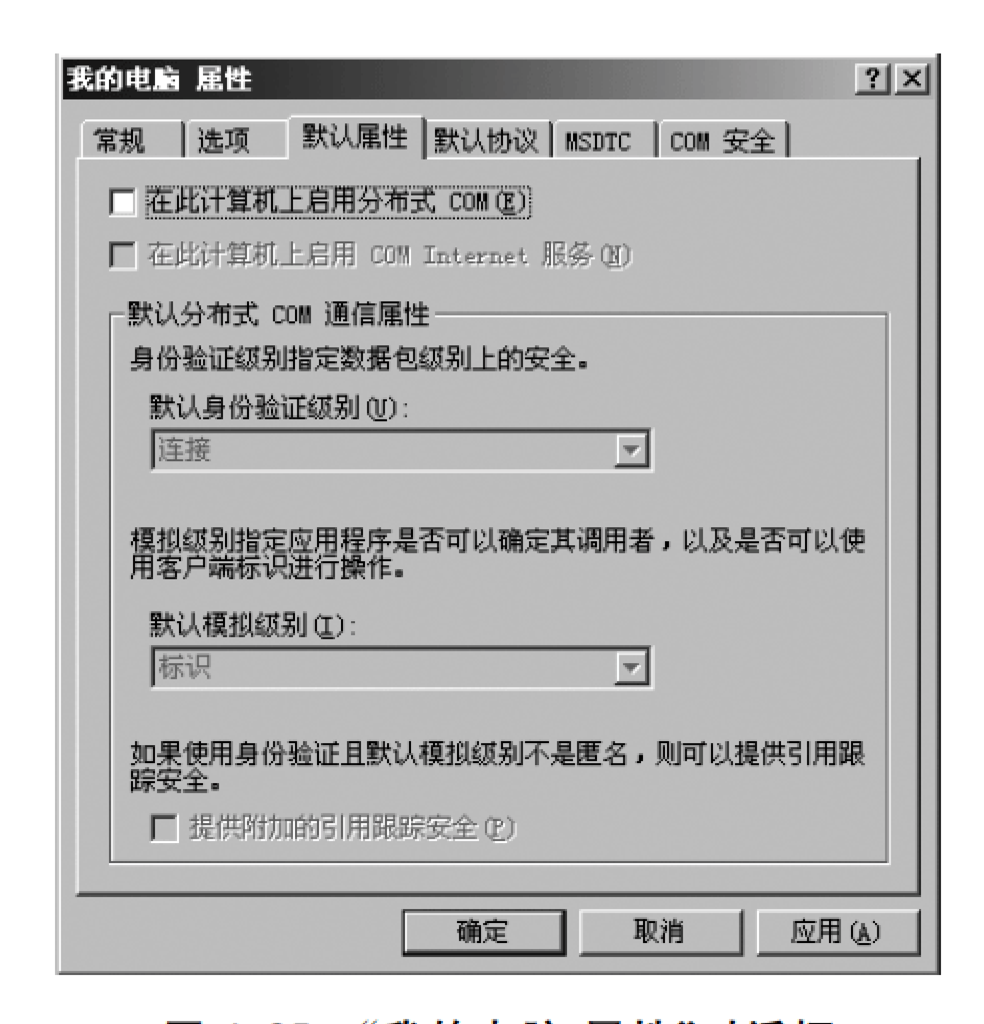


图 4.35 "我的电脑 属性"对话框



图 4.36 移除协议

重新启动之后即可关闭 135 端口。

(4) 关闭自动播放服务

自动播放功能不仅对光驱起作用，对其他驱动也起作用，这样很容易被黑客利用来执行黑客程序，因此，可以考虑关闭该服务。关闭自动播放服务的操作如下。

① 打开组策略编辑器，依次展开"计算机配置"→"管理模板"→"系统"。

② 双击右侧窗口中的"关闭自动播放"选项。

③ 在打开的对话框中选择"已启用"，然后在"关闭自动播放"后面的下拉菜单中选择"所有驱动器"选项，单击"确定"按钮即可生效。

另外,打开“本地连接”的 Windows Server 2003 自带的防火墙,可以屏蔽端口,基本可达到 IPSec 的功能。例如,只保留远程桌面服务器端口 3389、Web 服务器端口 80、FTP 服务器端口 21、邮件服务器端口 25、POP3 服务器端口 110、网页浏览端口 443 和 SQL 监听端口 1433 等有用的端口,将其余端口屏蔽掉。

把不必要的服务都禁止,尽管这些不一定能被攻击者利用得上,但是从安全规则和标准看,多余的东西就没有必要开启,这样还可减少一份安全隐患。对于个人用户而言,可以在各项服务属性设置中将要关闭的服务设为“禁用”,这样在下次重启服务后不需要的服务就关闭了。

Windows Server 2003 系统中还可以关闭如下不常用的服务。

- Computer Browser(维护网络上计算机的最新列表及提供这个列表)。
- Task scheduler(允许程序在指定时间运行)。
- Messager(传输客户端和服务器之间的 NET SEND 和警报器服务消息)。
- Distributed File System(局域网管理共享文件)。
- Distributed linktracking client(用于局域网更新连接信息)。
- Error reporting service(发送错误报告)。
- Microsoft Search(提供快速的单词搜索)。
- PrintSpooler(如果没有打印机可禁用)。
- Remote Registry(远程修改注册表)。
- Remote Desktop Help Session Manager(远程协助)。

6. 删除不安全的组件

一些 ASP 木马或一些恶意程序都会使用到 WScript. Shellt 和 Shell. application 这两个组件,采用如下方法可删除或卸载这两个组件:删除注册表[HKEY_CLASSES_ROOT\CLSID\{72C24DD5-D70A-438B-8A42-98424B88AFB8}]对应的 WScript. Shell;删除注册表[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540000}]对应的 Shell. application;利用 regsvr32/u wshom. ocx 卸载 WScript. Shell 组件;利用 regsvr32/u shell32. dll 卸载 Shell. application 组件。

7. 账户锁定设置

账户锁定策略是一项 Active Directory 安全功能。在指定时间段内,如果登录尝试失败次数达到指定次数,它会锁定用户账户并禁止登录。允许尝试的次数和时间段基于为账户锁定设置的值。账户锁定策略还可以指定锁定期限。账户锁定设置有助于防止攻击者猜测用户密码,并且会降低对网络环境攻击成功的可能性。

选择“开始”→“运行”命令,在出现的对话框中输入 secpol. msc,打开本地安全设置界面,选择“账户锁定策略”,如图 4.37 所示。双击账户锁定阈值,在出现的对话框中输入允许尝试的最大登录次数,确认即可。

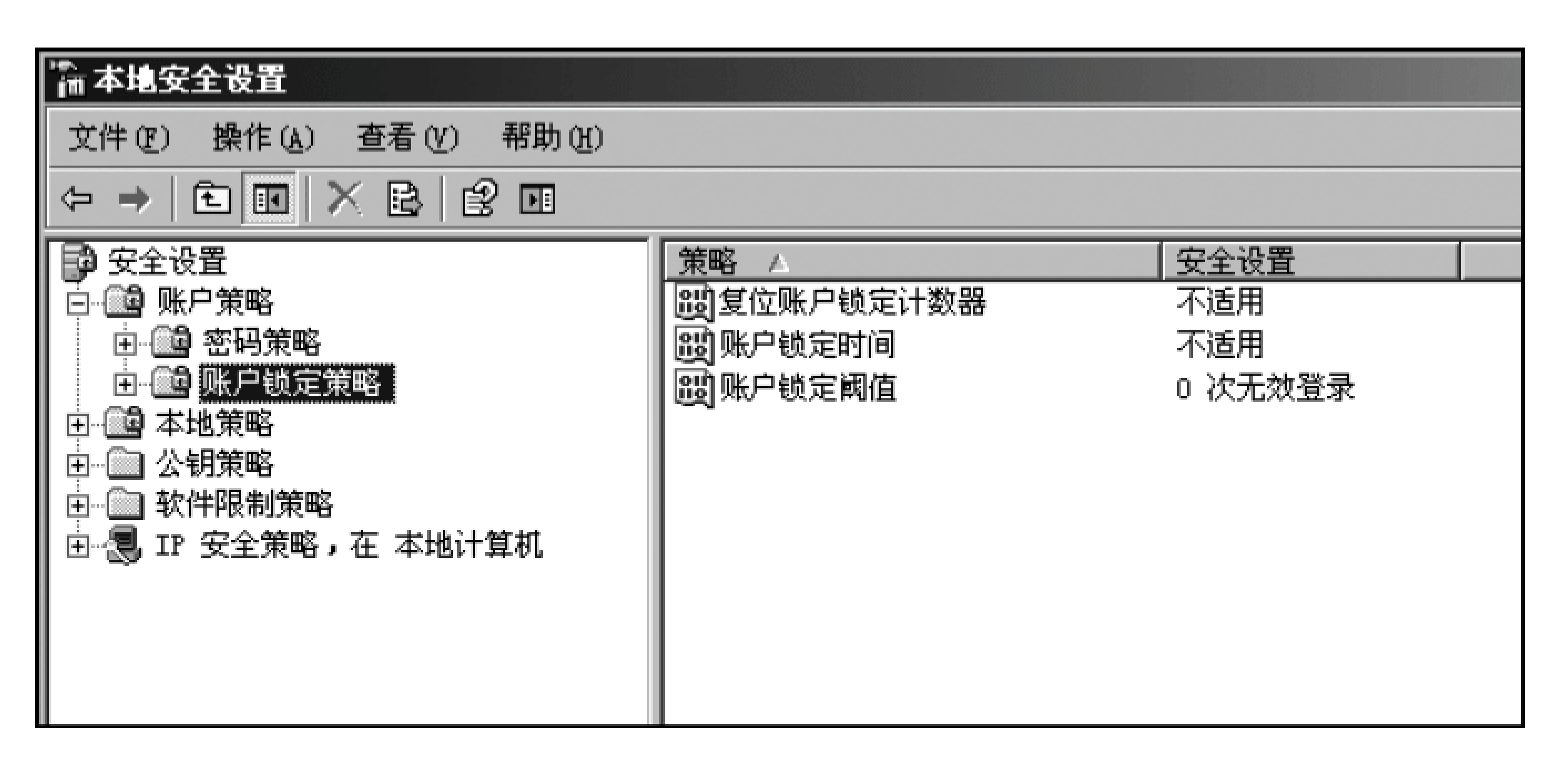


图 4.37 账户锁定策略

本 章 小 结

操作系统是信息系统最基本、最关键的系统软件，它为用户及其应用程序和硬件之间提供了一个接口，可对计算机进行有效、合理使用，并对资源进行管理和保护。

操作系统的安全表现在系统安全、用户安全、资源安全和通信安全等方面，其保证机制就是用户身份验证、授权访问和审计。

本章主要讲述了操作系统的安全性及安全配置、Windows Server 2003 中的用户管理及其策略、Windows Server 2003 中的文件访问权限及其策略、Windows Server 2003 中的资源审计及基本安全应用。

本 章 练 习

一、填空题

1. 操作系统安全主要包括________、________、________、________ 4 个方面的安全。

2. 操作系统的安全机制主要有________机制、________机制和________机制。

3. 安全策略的目标是____________________。

4. 安全策略主要包括________策略、________策略和________策略。

5. Windows Server 2003 的事件日志文件分为________、________、________、________ 4 大类。

二、选择题

1. 在 Windows Server 2003 系统中代表一个用户、组或计算机的符号是________。

A. AT　　B. SAD　　C. ACL　　D. SID

2. 在 Windows Server 2003 系统中要改变一个本地账户密码，则应________。
   A. 在用户管理嵌入式单元右击账户
   B. 在本地安全嵌入式单元右击账户
   C. 在本地安全策略嵌入式单元右击账户
   D. 在本地用户和组中，右击账户
3. 为了设置基于用户的本地文件权限，必须采用________文件系统。
   A. FAT　　B. NTFS　　C. UID　　D. GID
4. 没有启用 NTFS 之前，下面________功能不能用。
   A. 日志 T　　B. 删除文件　　C. 审核　　D. 建立用户共享
5. 在 Windows Server 2003 系统事件查看器中，6007 号事件意味着________。
   A. 一次不成功的登录　　B. 关机事件
   C. 一个不正当的关闭事件　　D. 一个错误的服务

三、简答题

1. 如何衡量操作系统的安全性？
2. 操作系统的安全机制有哪些？
3. 为什么要制定操作系统的安全策略？
4. 用户管理的主要任务是什么？
5. 用户账户管理的基本内容是什么？
6. 说出组的概念及其特点。
7. Windows Server 2003 中 NTFS 权限的有效权限规则是什么？
8. Windows Server 2003 中审核资源的基本方法有哪些？
9. 如何安全配置 Windows Server 2003？

实训　网络用户规划与管理

实训目的

(1) 规划用户账户和组账户用户：账户和组账户的命名；用户账户密码要求、登录时间与站点限制、主文件夹的位置及配置文件的设置；组账户的类型和成员范围及计算机位置。

(2) 掌握用户账户的管理和内置用户账户的使用。

(3) 掌握用户账户的安全策略设置。

(4) 掌握组账户的管理和内置组账户的使用。

实训环境

一台装有 Windows Server 2003 的计算机。

实训步骤

第 1 步 规划组和用户账户。

假设某公司的组织机构如图 4.38 所示。其中，销售部有部门经理 Mana-SA 和 5 个销售员，所有人员全天可以访问域控制器 DOM1。

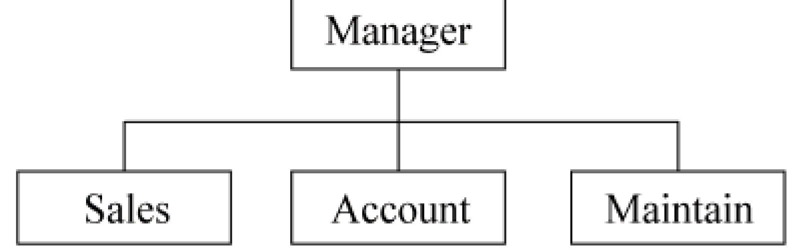


图 4.38 某公司组织机构

会计部有部门经理 Mana-AC 和 3 个财会人员，除部门经理外，其他财会人员只能在上午 8:00 到下午 5:00 访问数据库服务器 AC-DB。而且规定在站点为 ACWS1～ACWS4 的 4 台计算机登录。

维护部有部门经理 Mana-MA 和 4 个维护人员。有两个维护员在 7:00 到 18:59 登录，另两个维护员在 19:00 到 6:59 登录。只有部门经理可以备份数据。

请规划组和每个组的成员用户账户做出规划表，并就组和用户账户的安全提出有关密码和访问敏感数据的要求。

第 2 步 对组和用户账户的创建、修改或删除。

按照规划表的要求，请完成如下操作。

(1) 创建全局组 Sales、Account、Maintain 组和本地组 SA-users 和 ACC-users。

(2) 创建各组员的用户账户和用户 Manager。

(3) 把销售部的成员用户账户添加到 Sales 组，然后把全局组 Sales 添加到 SA-users 组，按要求在域控制器 DOM1 上给他们建立用户的主文件夹。

(4) 把会计部的成员账户添加到全局组 Account，并把该全局组添加到本地组 ACC-users 中，在数据库服务器上建立用户的主文件夹。

(5) 将维护部的成员用户账户添加到内置组 Users 和 Power Users。

(6) 将用户 Manager 添加到内置组 Administrators。

(7) 将维护部经理的用户账户加入 Backup 组。

(8) 修改销售部其中一个成员的用户账户，使其为临时人员，并设置其账户过期时间。

(9) 删除一个维护部人员的用户账户。

第 3 步 设置用户账户策略。

(1) 设置用户账户的密码策略

① 最小密码长度：7。

② 密码最长存留期：10 天。

③ 必须符合安装的密码筛选器的复杂性要求：启用。

④ 用户必须登录以后更改密码。

⑤ 强制密码历史：5 次。

(2) 设置用户账户策略

① 账户锁定阈值：3 次。

② 账户锁定时间：20 分钟。

③ 复位锁定计数：20 分钟。

第 5 章

防火墙技术

Chapter 5

知识目标

- 掌握防火墙的概念、功能特点及安全性。
- 掌握防火墙的分类。
- 了解防火墙的选购、安装和维护。
- 掌握常用防火墙系统结构。

技能目标

- 能够识别防火墙系统基本结构。
- 能够利用天网防火墙进行网络安全设置。
- 掌握瑞星防火墙的使用。

企业的内部网与 Internet 相连，方便了企业内部之间及企业与外部的信息交流，提高了工作效率。然而，一旦企业内部网连入 Internet，就意味着 Internet 上的每个用户都有可能访问企业网。如果没有一个安全性保护措施，黑客可能会在毫无察觉的情况下进入企业网，非法访问企业的资源。而防火墙（firewall）就是保护企业内部网中信息安全的一项重要措施。

5.1 防火墙技术简介

防火墙是一种能将内部网和公众网分开的方法。它能限制被保护的网络与 Internet 及其他网络之间进行的信息存取、传递等操作。在构建安全的网络环境过程中，防火墙作为第一道安全防线，正受到越来越多用户的关注。

5.1.1 防火墙的定义

“防火墙”原来是指在建筑物中用来隔离不同的房间，防止火灾蔓延的隔断墙，现在人们引用这个概念，把用于保护计算机网络中敏感数据不被窃取和篡改的计算机软/硬系统叫作“防火墙”。

防火墙是设置在不同网络（如可信任的企业内部网和不可信任的公共网）或网络安全域之间的一系列部件的组合。它可通过监测、限制、更改跨越防火墙的数据流，尽可能地

对外部屏蔽网络内部的信息、结构和运行状况,以此来实现网络的安全保护。

防火墙实际上是一种访问控制技术,它在一个被认为是安全和可信的内部网络和一个被认为是不那么安全和可信的外部网络之间设置障碍,阻止对信息资源的非法访问,也可以阻止保密信息从受保护网络上被非法输出。它能允许你"同意"的人和数据进入你的网络,同时将你"不同意"的人和数据拒之网外。换句话说,如果不通过防火墙,可信网络内部和外部的人就无法进行通信。

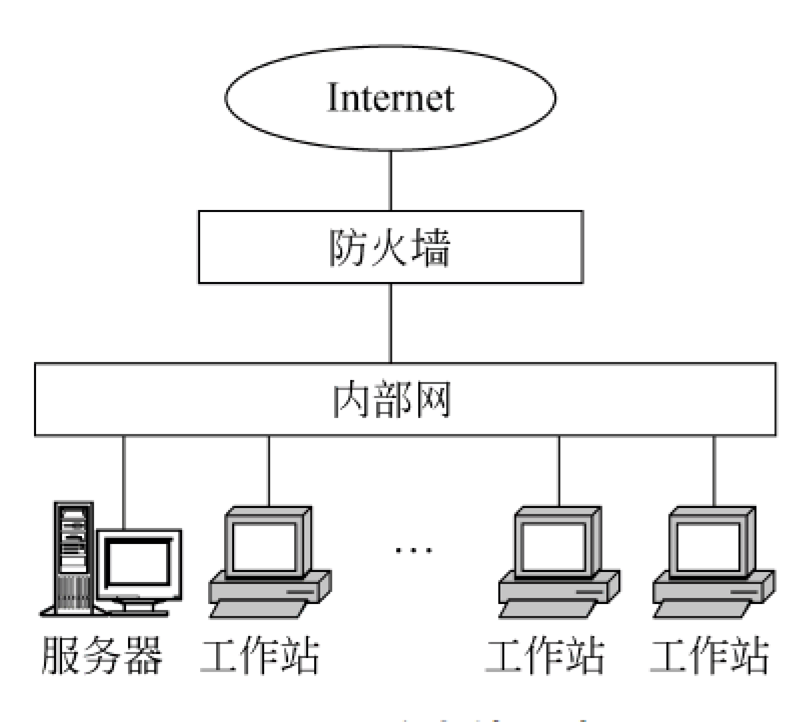


图 5.1　防火墙示意

防火墙是一类防范措施的总称,不是一个单独的计算机程序或设备。在物理上,它通常是一组硬件设备和软件的多种组合。在逻辑上,它是分离器、限制器和分析器,可有效地监控内部网和公共网之间的任何活动。防火墙是不同网络或网络安全域之间信息的唯一出入口,能根据一定的安全政策控制出入网络的信息流。防火墙本身具有较强的抗攻击能力,是提供信息安全服务、实现网络和信息安全的基础设施。图 5.1 为防火墙示意。

5.1.2　防火墙的功能

一方面,防火墙对经过它的网络通信进行扫描,过滤一些可能攻击内部网络的数据;另一方面,防火墙可以关闭不使用的端口,能禁止特定端口通信,封锁特洛伊木马。它可以禁止来自特殊站点的访问,从而防止来自不明入侵者的所有通信。具体来说,防火墙的功能主要体现在以下几个方面。

1. 防火墙是网络安全的屏障

一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性,并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙,所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络,这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击,如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置,能将所有安全软件(如口令、密码、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比,防火墙的集中安全管理更经济。如在网络访问时,口令系统和其他的身份认证系统完全不必分散在各个主机上,而是集中在防火墙身上。

3. 进行网络存取和访问监控审计

如果所有的访问都经过防火墙,那么,防火墙就能记录下这些访问并作出日志记录。

当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是非常重要的，它可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。而网络使用统计对网络需求分析和威胁分析等而言也是非常重要的。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现对内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局造成的影响。再者，隐私是内部网络非常关心的问题，一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣，甚至因此暴露了内部的某些安全漏洞。使用防火墙就可以隐蔽一些能透露内部细节的服务，如 Finger、DNS 等。Finger 显示的信息非常容易被攻击者所获悉，攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时引起注意等。防火墙可以同样阻塞有关内部网络中的 DNS 信息，这样一台主机的域名和 IP 地址就不会被外界所了解。

5. 支持具有 Internet 服务特性的企业内部网络技术体系

通过企业内部网络技术体系(VPN)，将企事业单位分布在全世界各地的 LAN 或专用子网，有机地连成一个整体，不仅省去了专用通信线路，而且为信息提供了技术保障。

尽管防火墙有许多防范功能，但由于 Internet 的开放性，它也有一些不尽如人意的地方，主要表现在以下几个方面。

(1) 防火墙不能防范绕过防火墙的攻击。例如，在一个被保护的网络上有一个没有限制的拨出存在，内部网上的用户就可以直接通过 SLIP 或 PPP 连接进入外部网络。内部网络用户可能会对需要附加论证的代理服务器感到厌烦，因而通过 SLIP 或 PPP 连接 Internet，从而试图绕过由精心构造的防火墙系统提供的安全系统，这就为从后门攻击创造了极大的可能。网络上的用户必须了解，这种类型的连接对于一个有全面的安全保护系统来说是绝对不允许的。

(2) 防火墙不能防止数据驱动式攻击。当有些表面看来无害的数据被邮寄或复制到 Internet 主机上并被执行而发起攻击时，就会发生数据驱动攻击。例如，一种数据驱动的攻击可以使一台主机修改与安全有关的文件，从而使得入侵者很容易获得对系统的访问权，以便下一次更容易地入侵该系统。

(3) 防火墙不能防止感染病毒的软件或文件的传输。这是因为病毒的类型太多，操作系统也有多种，编码与压缩二进制文件的方法也各不相同，所以不能期望 Internet 防火墙去对每一个文件进行扫描，查出潜在的病毒。对病毒特别关心的机构应在每个桌面部署防病毒软件，防止病毒从软盘或其他来源进入网络系统。

(4) 防火墙不能防止来自内部变节者和用户带来的威胁。防火墙无法禁止变节者或内部存在的间谍将敏感数据拷贝，并将其带出。防火墙也不能防范有人故意伪装成超级用户，劝说没有防范心理的用户公开口令或授予其临时的网络访问权限。

防火墙只是整体安全防范政策的一部分。整个网络易受攻击的各个点必须以相同程度的安全防护措施加以保护。

5.1.3 防火墙技术的发展趋势

网络安全通常是通过技术与管理两者相结合来实现的,良好的网络管理加上优秀的防火墙技术是提高网络安全性能的最好选择。虽然网络防火墙技术已经发展了几代,防火墙的研究和开发人员也已尽了很大努力,但用户的需求永远是推动技术前进的原动力。

随着网上的攻击手段不断出现,以及防火墙在用户的核心业务系统中占据的地位越来越重要,用户对防火墙的要求越来越高。如用户可能要求防火墙应能提供更细粒度的访问控制手段,防火墙对新出现的漏洞和攻击方式应能够迅速提供有效的防御办法,防火墙的管理应更加容易和方便,防火墙在紧急情况下可以做到迅速响应,防火墙具有很好的性能和稳定性等。用户的这些要求归纳起来是防火墙技术应具备智能化、高速度、分布式并行结构、多功能和专业化的发展趋势。

1. 智能化

防火墙将从目前的静态防御策略向具备人工智能化方向发展。未来智能化的防火墙应能实现以下功能。

(1) 自动识别并防御各种黑客攻击手法及其相应变种攻击手法。

(2) 在网络出口发生异常时自动调整与外网的连接端口。

(3) 根据信息流量自动分配、调整网络信息流量及协同多台物理设备工作。

(4) 自动检测防火墙本身的故障并能自动修复。

(5) 具备自主学习并制定识别与防御方法。

2. 高速度

随着网络传输速率的不断提高,防火墙必须在响应速度和报文转发速度方面做相应的升级,这样才不至于成为网络的瓶颈。

3. 分布式并行结构

分布式并行处理的防火墙是防火墙的另一发展趋势,在这种概念下,将有多台物理防火墙协同工作,共同组成一个强大的、具备并行处理能力和负载均衡能力的逻辑防火墙。

4. 多功能

未来网络防火墙将在现有基础上继续完善其功能并不断增强新的功能,具体如下。

(1) 在保密性方面,将继续发展高保密性的安全协议用于建立 VPN,基于防火墙的 VPN 在较长一段时间内将继续成为用户使用的主流。

(2) 在过滤方面,将从目前的地址、服务、URL、文本、关键字过滤发展到多 CGI、Active、Java 等 Web 应用的过滤,并将逐渐具备病毒过滤的功能。

(3) 在服务方面,将在目前透明应用的基础上完善其性能,并将具备针对大多数网络通信协议的代理服务功能。

(4) 在管理方面,将从子网和内部网络的管理方式向基于专用通道和安全通道的远

程集中管理方式发展;管理端口的安全性将是其重点考虑的内容;用户费用统计、多种媒体的远程警报及友好的图形管理界面将成为防火墙的基本功能模块。

(5) 在安全方面,对网络攻击的检测、拦截及告警功能将继续是防火墙最主要的性能指标。

5. 专业化

单向防火墙、电子邮件防火墙、FTP 防火墙等针对特定服务的专业化防火墙将作为一种产品门类出现。

未来防火墙的发展思路将是:防火墙从目前对子网或内部网管理的方式向远程上网集中管理的方式发展;过滤深度不断加强,从目前的地址、服务器过滤,发展到 URL(页面)过滤、关键字过滤和对 Activex、Java 等的过滤,并逐渐有病毒清除功能。利用防火墙建立 VPN 是较长一段时间内用户使用的主流,IP 的加密需要越来越强,安全协议的开发是一大热点;对网络攻击的检测和告警将成为防火墙的重要功能。此外,网络的防火墙产品还将把网络前沿技术,如 Web 页面超高速缓存、虚拟网络和带宽管理等与其自身结合起来。



【案例】 天网防火墙系统设置

操作步骤

第 1 步 安装天网防火墙之后,打开“天网防火墙个人版”窗口,如图 5.2 所示。



图 5.2 “天网防火墙个人版”窗口

注意: 由于防火墙一般都要检查网络连接,因此,在自己的计算机上安装网络防火墙后,上网速度可能会有所下降,但并不明显。

第2步 右击桌面右下角的“天网防火墙”图标，并在弹出的快捷菜单中选择“退出”命令，即可退出“天网防火墙个人版”程序。

第3步 单击主窗口中的“应用程序规则”按钮，即可打开“应用程序规则”对话框，从中可以设置允许(√)、提示(?)、禁止(×)3种方式来判断是否允许访问网络资源，如图5.3所示。

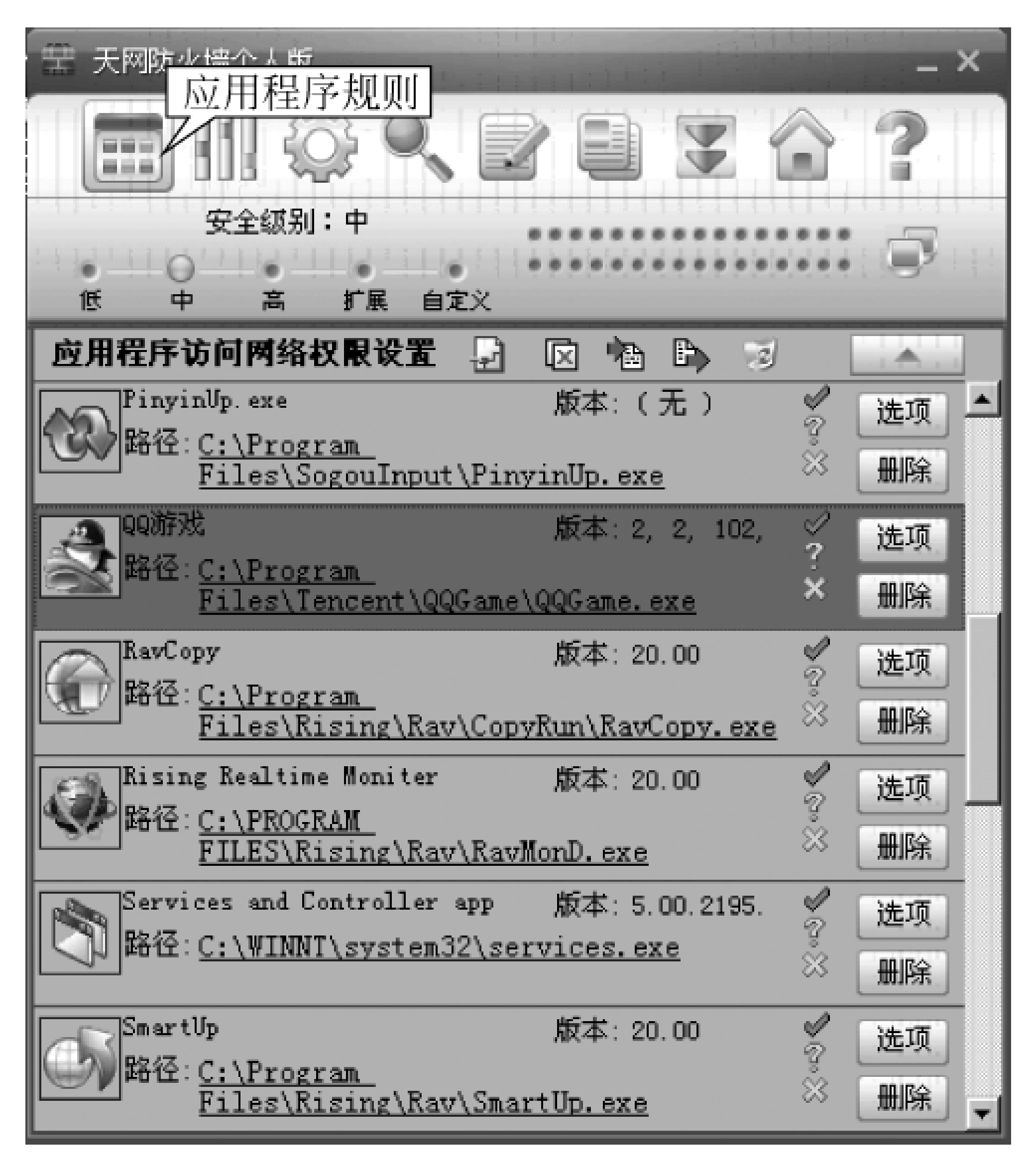


图5.3 设置应用程序规则

第4步 选择其中一个程序(如“QQ游戏”)，单击“删除”按钮，即可打开“天网防火墙提示信息”对话框，如图5.4所示。

第5步 单击“确定”按钮之后，将禁止QQ游戏使用网络资源，如果此时再运行QQ游戏，将打开“天网防火墙警告信息”对话框，如图5.5所示。只有取消选中“该程序以后

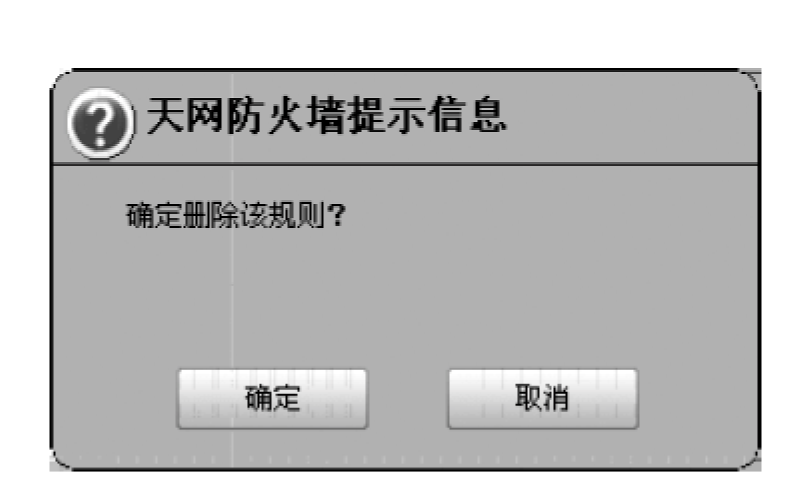


图5.4 天网防火墙提示信息

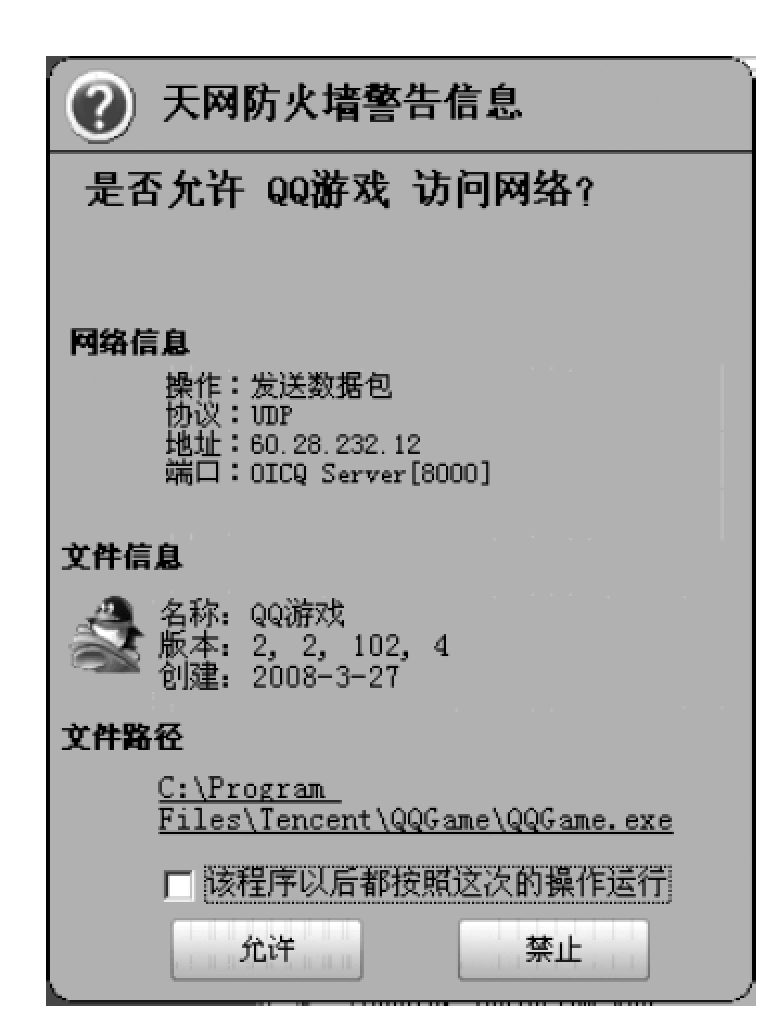


图5.5 天网防火墙警告信息

都按照这次的操作运行”复选框并单击“允许”按钮，该 QQ 游戏程序才可以使用网络资源。

注意：应用程序中的“√”表示该程序可以使用网络资源；“?”表示该程序使用网络资源时将弹出信息提示对话框；“×”表示该程序不能使用网络资源。如已经禁止了 QQ 游戏程序，则运行 QQ 游戏时，将显示无法连接。

第 6 步　在“应用程序规则”对话框选择一项并双击“选项”按钮，即可打开“应用程序规则高级设置”对话框，如图 5.6 所示。

第 7 步　如果选择“端口范围”单选按钮，从中即可设定该程序访问网络的端口范围(本对话框中内容表示 Firefox 程序只能使用 0～1024 的端口)，如图 5.7 所示。

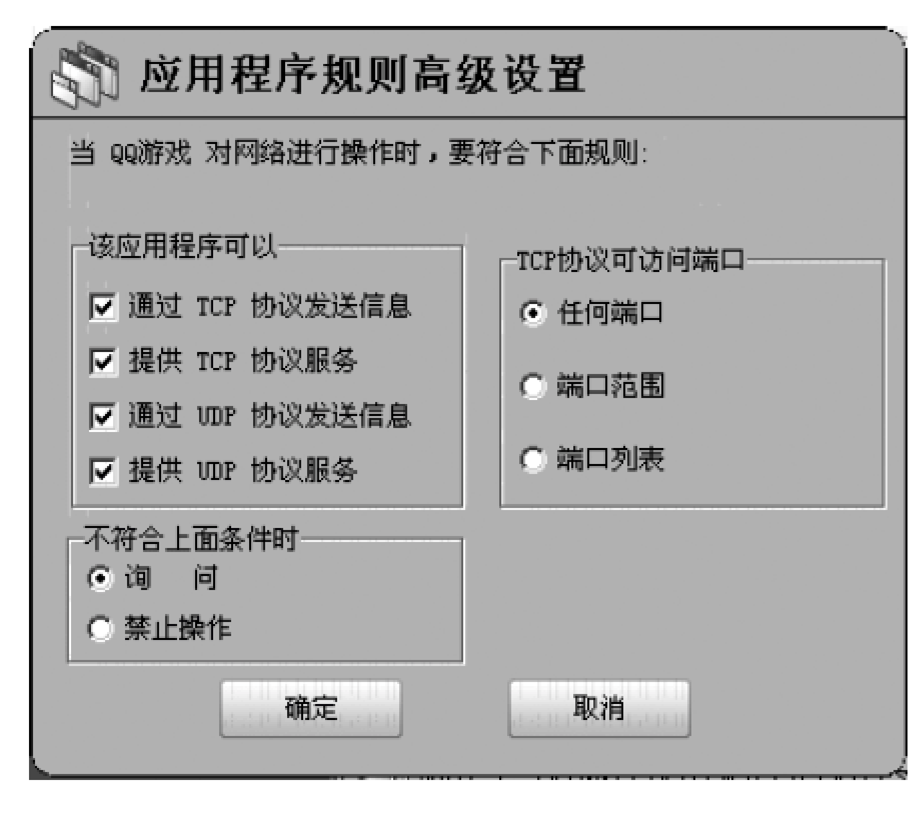


图 5.6　“应用程序规则高级设置”对话框

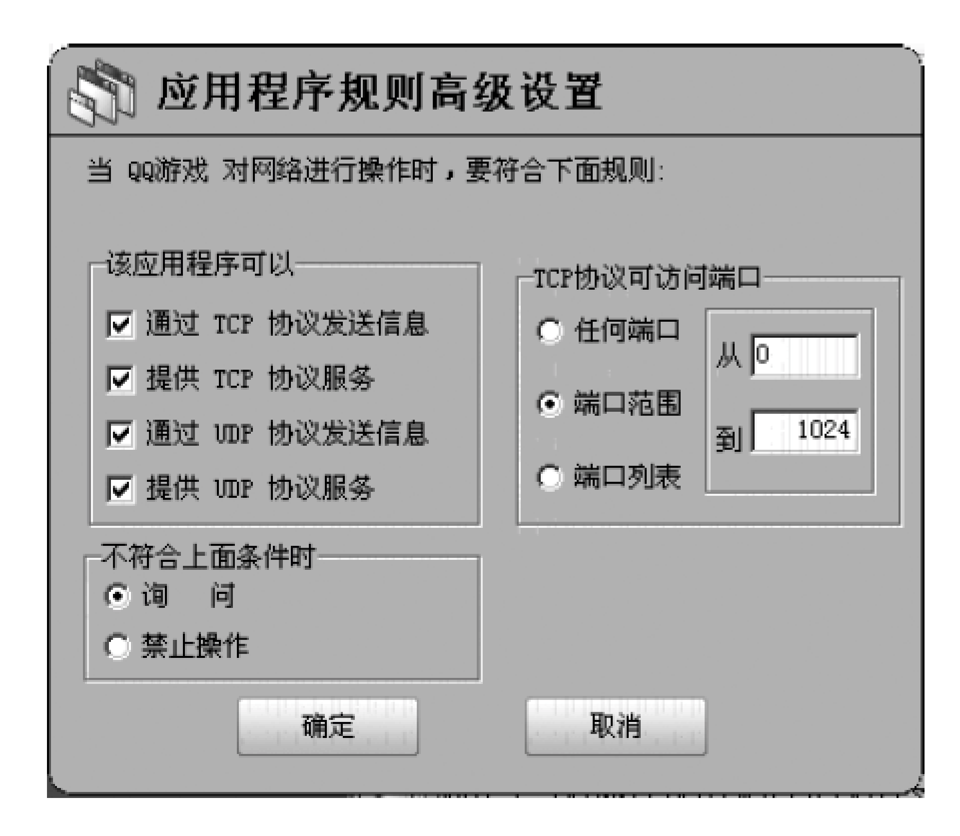


图 5.7　设置端口范围

第 8 步　选择“端口列表”单选按钮，在右侧列表框处列出了该程序可使用的端口，如图 5.8 所示。

第 9 步　在“应用程序规则”对话框单击“IP 规则管理”按钮，即可打开“自定义 IP 规则”对话框，选择其中任一项，即可在列表框中出现对该规则的描述，如图 5.9 所示。



图 5.8　设置端口列表

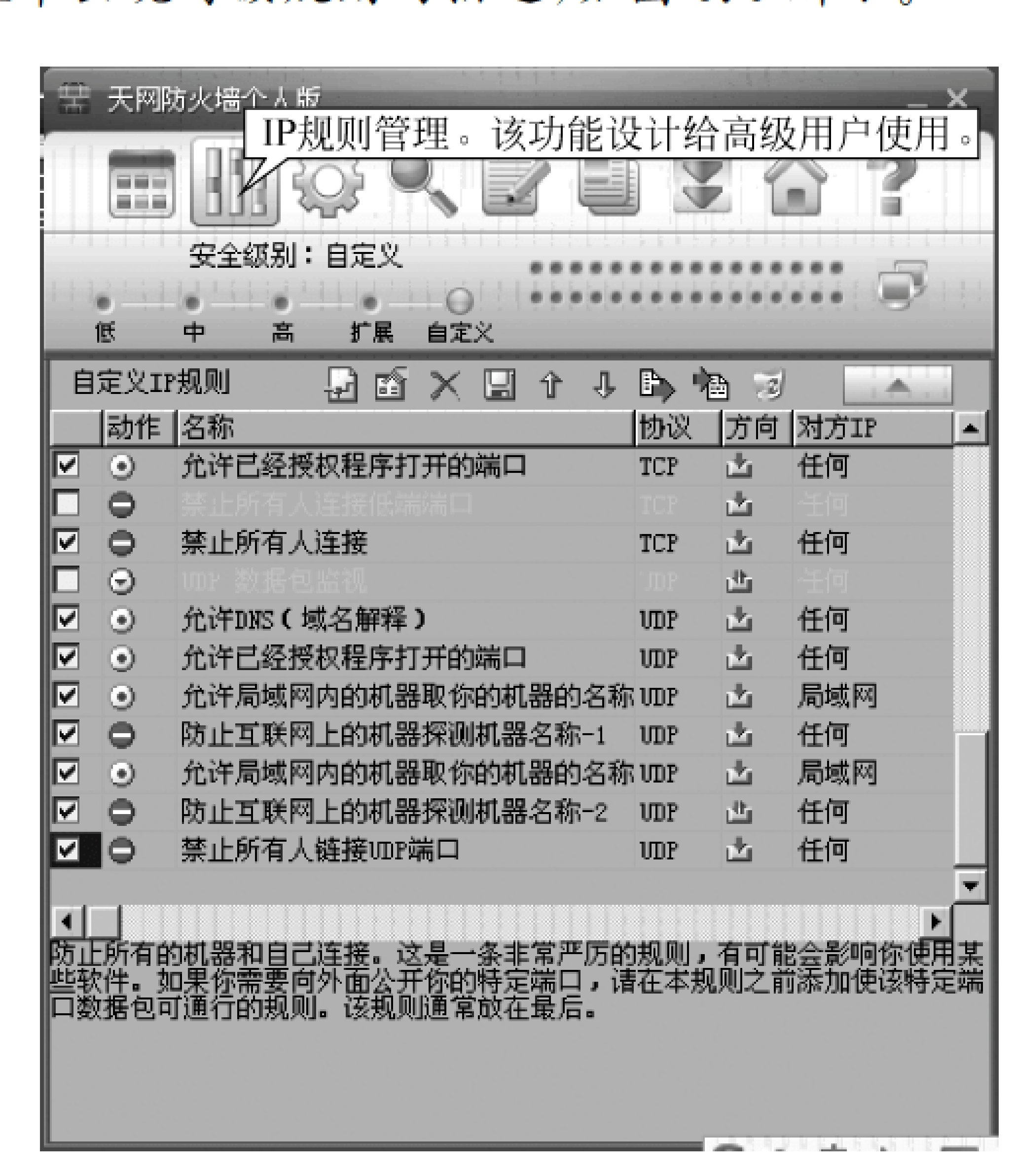


图 5.9　自定义 IP 规则

第 10 步 在“应用程序规则”对话框单击“系统设置”按钮并选中“启动”选项组中的“开机后自动启动防火墙”复选框，则以后每次启动计算机时都将自动运行天网防火墙。如果单击“重置”按钮，则会打开图 5.10 所示的对话框。单击“确定”按钮，即可删除所有后来加入的新规则，而所有被修改的规则都将变成初始的默认设置。



图 5.10 设置提示信息

第 11 步 单击“向导”按钮，即可打开“天网防火墙设置向导”窗口，如图 5.11 所示。



图 5.11 “天网防火墙设置向导”窗口

第 12 步 单击“下一步”按钮，即可进入“安全级别设置”对话框，从中选择所要使用的安全级别，如图 5.12 所示。

我要使用的安全级别是
○低 ◉中 ○高 ○自定义

图 5.12 设置安全级别

第 13 步 单击“下一步”按钮，即可进入“常用应用程序设置”对话框，在其中可以选择防火墙允许访问网络的程序。

第 14 步 单击“下一步”按钮，即可进入“局域网信息设置”对话框。其中选中“开机的时候自动启动防火墙”复选框，即可让防火墙在开机的时候自动开始对计算机进行保护。在“我的局域网的地址是”文本框中，只要输入要设定的 IP 地址即可。

第 15 步 在完成设置之后，单击“结束”按钮，即可完成对天网防火墙的系统设置。

5.2 防火墙技术的分类

防火墙是近期发展起来的一种保护计算机网络安全的技术性措施，它是一个用来阻止网络中的黑客访问某个机构网络的屏障，在网络边界上通过建立起来的相应网络监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。目前的防火墙主要有两大类：包过滤防火墙和代理防火墙。

5.2.1 包过滤防火墙技术

1. 包过滤防火墙技术

数据包过滤(packet filtering)技术是防火墙为系统提供安全保障的主要技术，它依据系统内事先设定的过滤逻辑，通过设备对进出网络的数据流进行有选择地控制与操作。

数据包过滤技术作为防火墙的应用有 3 种。第一种是路由设备在完成路由选择和数据转发的同时进行包过滤。第二种是在工作站上使用软件进行包过滤。第三种是在一种称为屏蔽路由器的路由设备上启动包过滤功能。目前较常用的方式是第一种。用户可以设定一系列的规则，指定允许哪些类型的数据包可以流入或流出内部网络，哪些类型的数据包的传输应该被拦截。

包过滤作用在网络层和传输层，以 IP 包信息为基础，对通过防火墙的 IP 包的源、目的地址，TCP/UDP 的端口标识符及 ICMP 等进行检查。规定了哪些网络节点何时可通过防火墙访问外部网络，哪些网络节点可访问内部网络。或者哪些用户只能使用电子邮件，而不能使用 Telnet 和 FTP，哪些用户只能使用 Telnet，而不能使用 FTP 等。可以利用安全策略形式语言描述安全配置规则，并进行一致性检查，达到灵活、方便地配置安全策略的目的。

包过滤规则检查数据流中的每个数据包后，根据规则来确定是否允许数据包通过，其核心是过滤算法的设计。如果包的出入接口相匹配，并且规则允许该数据包通过，那么该

数据包就会按照路由表中的信息被转发。但是,如果包的出入接口相匹配,而规则拒绝该数据包,那么该数据包也会被丢弃。如果出入接口未设匹配规则,用户配置的默认参数会决定是转发还是丢弃数据包。

数据包过滤在网络中起着举足轻重的作用,它允许用户在某个地方为整个网络提供特别的保护。例如,Telnet 服务器在 TCP 的 23 号端口上监听远程连接,为了阻塞所有进入的 Telnet 连接,包过滤路由器只需要简单地丢弃所有 TCP 端口号等于 23 的数据包。为了将进来的 Telnet 连接限制内部的数台机器上,包过滤路由器必须拒绝所有 TCP 端口号等于 23,并且目标 IP 地址不等于允许主机的 IP 地址的数据包。

包过滤的操作可以在路由器上进行,也可以在网桥,甚至在一个单独的主机上进行,大多数数据包过滤系统不处理数据本身,它们不根据数据包的内容做决定。

2. 包过滤防火墙技术的优缺点

数据包过滤防火墙技术有很多优点,主要体现在以下几点。

(1) 包过滤技术不用改动客户机和主机上的应用程序,因为过滤发生在网络层和传输层,与应用无关。

(2) 单独的、放置恰当的数据包过滤路由器有助于整个网络。如果仅有一个路由器连接内部网络和外部网络,那么不论网络大小、拓扑结构如何,所有网络通信都要通过那个路由器进行数据包过滤,这样在网络安全方面就能取得较好的效果。

(3) 数据包过滤技术对用户没有特别的要求。数据包过滤是在 IP 层实现的,它不要求任何自定义的软件或者特别客户机配置,也不要求用户经过任何特殊训练。当数据包过滤路由器在检查数据包时,它与普通路由器没什么区别,甚至用户感觉不到它的存在,除非用户试图做一些数据包过滤路由器所禁止的事。这样,对用户来说,数据包过滤技术具有较强的透明度,使用起来很方便。

(4) 大多数路由器都具有数据包过滤功能,不论是商业的还是免费的,许多硬件或软件路由产品都具有数据包过滤能力,大多数网络使用的路由器也具有这种功能,数据包过滤路由器工作时一般只检查报头相应的字段,而不查看数据包的内容,而且有些核心部件是由专用硬件实现的,所以转发速度快,效率比较高。

由以上优点可以看出,数据包过滤是一种通用、廉价、有效的安全手段,说它通用是因为它不针对各个具体的网络服务采取特殊的处理方式。说它廉价是因为大多数路由器都提供分组过滤功能。说它有效是因为它能在很大程度地满足企业的安全要求。

数据包过滤存在的缺陷主要体现在以下几点。

(1) 在过滤过程中判别的只有网络层和传输层的有限信息,而不能在用户级别上进行过滤,不能识别不同的用户和防止 IP 地址的盗用,因而各种安全要求不可能得到充分满足。例如,攻击者可以把自己主机的 IP 地址设成一个合法主机的 IP 地址,这样就可以很轻易地通过报文过滤器。

(2) 在许多过滤器中,过滤规则的数目是有限制的,随着规则数目的增加,设备性能会受到很大的影响,导致数据包过滤器使用户难以使用某些需要的规则。例如,用户只能确定数据包来自什么主机,而不能指定到达特定的应用程序;当用户通过端口号对一些协

议实行限制时，其他的协议同时也被禁止了。

(3) 当前的过滤工具并不完善，或多或少地存在一些局限性。如数据包过滤规则难以配置，甚至不可能运行；难以检查数据包过滤规则；许多产品的数据包过滤能力不完全等。

(4) 由于缺少上下文关联信息，数据包过滤路由器不能有效地过滤诸如 UDP、RPC、FTP 一类的协议。

(5) 数据包过滤技术对安全管理人员素质要求较高。建立安全规则时，管理人员必须对协议本身及其在不同应用程序中的作用有较深入的理解。

在实际应用中，很少把数据包过滤技术当成单独的安全解决方案，主要是因为数据包过滤技术本身的缺陷。过滤路由器通常是和应用网关配合或是与其他防火墙技术一起使用，共同组成防火墙系统。

5.2.2 代理防火墙技术

1. 代理防火墙技术

代理防火墙即代理服务器(proxy server)。代理服务器是指代理内部网络用户与外部网络服务器进行信息交换的程序。它可以将内部用户的请求确认后送达外部服务器，同时将外部服务器的响应再送给用户。这种技术经常被用于在 Web 服务器上高速缓存信息，扮演着 Web 客户和 Web 服务器之间的中介角色。它主要保存 Internet 上最常用和最近访问过的内容，可为用户提供更快的访问速度，并且提高了网络安全性。由于代理服务器在外部网络向内部网络申请服务时发挥了中间转接和隔离的作用，因此，又把它叫作代理防火墙。

代理防火墙作用在应用层，用来提供应用层服务的控制，其特点是完全阻隔了网络通信流，通过对每种应用服务编制专门的代理程序。实现监视和控制应用层通信流的作用。所以代理防火墙又被称为应用代理或应用层网关型防火墙。

应用层网关型防火墙控制的内部网络只接受代理服务器提出的服务请求，拒绝外部网络其他接点的直接请求。它同时提供了多种方法认证用户。当确认了用户名和口令后，服务器根据系统的设置对用户作进一步的检查，验证其是否可以访问本服务器。应用层网关型防火墙还对进出防火墙的信息进行记录，并可由网络管理员用来监视和管理防火墙的使用情况，实际中的应用网关通常由专用代理服务器实现。图 5.13 为代理防火墙的示意图。

具体来说，应用层网关是内部网与外部网的隔离点，掌握着应用系统中可用做安全决策的全部信息。这使网络管理员能够实现比包过滤路由器更严格的安全策略。应用层网关不用依赖包过滤工具来管理 Internet 服务在防火墙系统中进出，而是采用为每种所需服务安装特殊代码的方式来管理 Internet 服务。如果网络管理员没有为某种应用安装代理编码，那么该项服务就不支持并不能通过防火墙系统来转发。同时，代码还可以配置成只支持网络管理员认为必需的部分功能，从而有效地防止网络攻击。

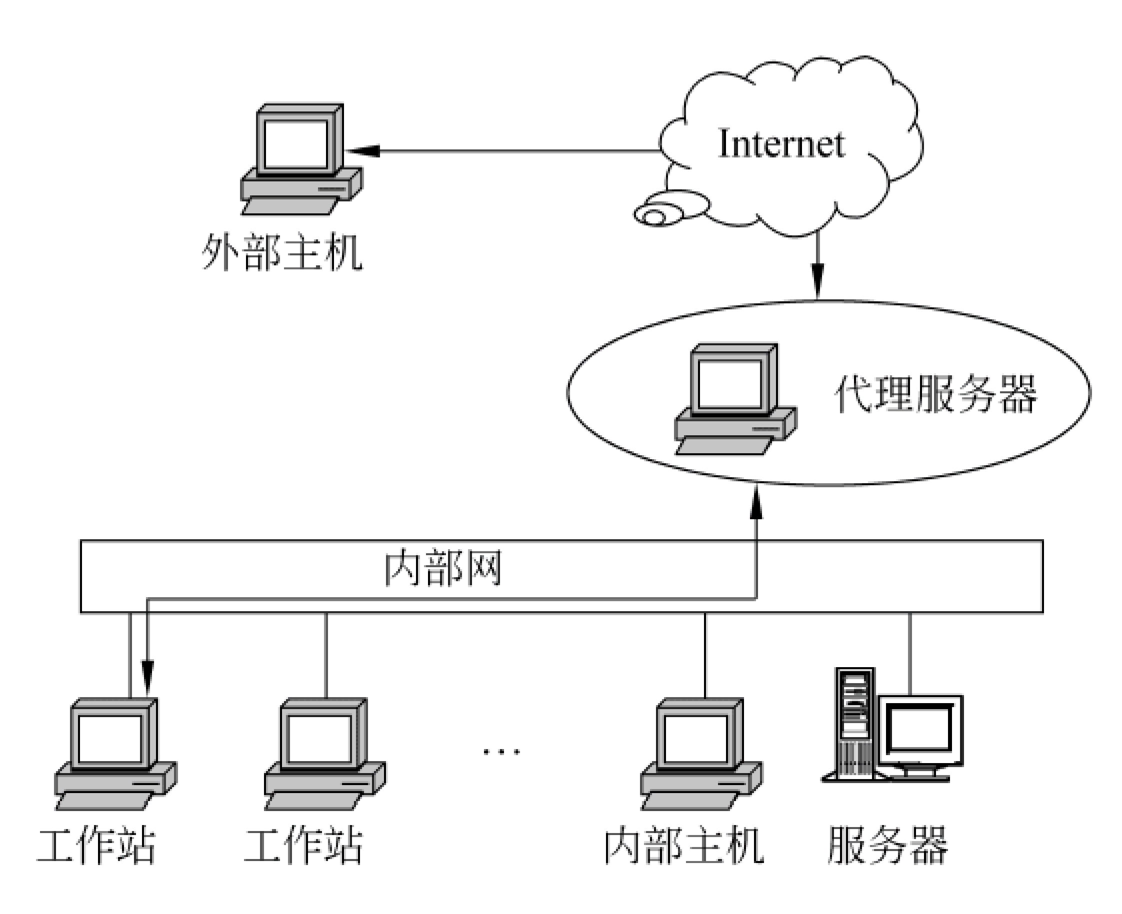


图 5.13　代理防火墙示意

2. 代理防火墙技术的优缺点

(1) 代理防火墙技术的优点

① 代理能生成各项记录。因为代理工作在应用层,它检查各项数据,可以按一定准则让代理生成各项日志、记录。这些日志、记录对于流量分析、安全检验是十分重要和宝贵的,当然,它们也可以用于计费等。

② 代理易于配置。代理因为是一个软件,所以它较路由器更易配置。配置界面十分友好。如果代理实现得好,可以对配置协议要求较低,从而避免了配置错误。

③ 代理能灵活、完全地控制进出流量、内容。通过采取一定措施,按照一定的规则,用户可以借助代理实现一整套的安全策略。比如可控制谁和什么时间和地点。

④ 代理能过滤数据内容。用户可以把一些过滤规则应用于代理,让它在高层实现过滤功能,如文本过滤、图像过滤(目前还未实现,但这是一个热点研究领域)、预防病毒或扫描病毒等。

⑤ 代理可以方便地与其他安全手段集成。目前的安全问题解决方案很多,如认证、授权、账户、数据加密、安全协议等。如果把代理与这些手段联合使用,将大大增加网络安全性。

(2) 代理防火墙技术的缺点

① 代理对用户不透明,大多代理要求客户端做相应改动或安装定制客户端软件,这给用户增加了不透明度。为庞大的互联网中的每一台内部主机安装和配置特定的应用程序既消耗时间,又容易出错,因为它们的硬件平台和操作系统都存在差异。

② 代理速度比路由器慢。路由器只是简单查看 TCP/IP 报头,检查特定的几个域,不做详细分析、记录,而代理工作于应用层,要检查数据包的内容,按特定的应用协议进行审查,扫描数据包内容,并进行转发请求,或响应,所以启动速度较慢。

③ 对于每项服务代理可能要求不同的服务器。可能需要为每项协议设置一个不同的代理服务器。因为代理服务器不得不理解协议以便判断什么是允许的和不允许的,并

且还装扮成一个对真实服务器来说是客户，对代理客户来说是服务器的角色，挑选、安装和配置所有这些不同服务器也可能是一项较复杂的工作。

④ 除了一些为代理而设的服务，代理服务器要求对客户或过程进行限制，每一种限制都有不足之处，人们无法经常按自己的步骤使用快捷、可用的工作。由于这些限制，代理应用就不能像非代理应用运行得那么好，它们往往可能曲解协议的说明，并且一些客户和服务器比其他的要缺少一些灵活性。

⑤ 代理服务器不能保证免受所有协议弱点的限制。作为一个安全问题的解决方法，代理取决于对协议中哪些是安全操作的判断能力。每个应用层协议，都或多或少存在一些安全问题，对于一个代理服务器来说，要彻底避免这些安全隐患几乎是不可能的，除非关掉这些服务。代理取决于在客户端和真实服务器之间插入代理服务器的能力，这要求两者之间交流的相对直接性。而且有些服务的代理是相当复杂的。

⑥ 代理不能改进底层协议的安全性。因为代理工作于应用层，所以它就不具备改善底层通信协议的能力。而这些方面，对于一个网络的健壮性是相当重要的。

在实际应用中，构筑防火墙的解决方案很少采用单一的技术，大多数防火墙是将数据包过滤和代理服务器结合起来使用的。

5.3 防火墙的基本体系结构

出于对更高安全性的要求，通常的防火墙系统是多种解决不同问题的技术的有机组合。例如，把基于包过滤的方法与基于应用代理的方法结合起来。就形成复合型防火墙产品。目前常见的有以下几种配置方法。

1. 屏蔽路由器

屏蔽路由器是防火墙最基本的构件，是最简单也是最常见的防火墙。屏蔽路由器作为内外连接的唯一通道，要求所有的报文都必须在此通过检查。路由器上可以安装基于IP层的报文过滤软件，实现报文过滤功能。许多路由器本身带有报文过滤配置选项，但一般比较简单。

这种配置的优点是：容易实现、费用少，并且对用户的要求较少，使用方便。其缺点是：日志记录能力不强，规则表庞大、复杂，整个系统依靠单一的部件来进行保护，一旦被攻击，系统管理员很难确定系统是否正在被入侵或已经被入侵了。

2. 双宿主主机网关

双宿主主机是一台安装有两块网卡的计算机，每块网卡有各自的IP地址，并分别与受保护网和外部网相连。如果外部网络上的计算机想与内部网络上的计算机进行通信，它就必须与双宿主主机上与外部相连的IP地址联系，代理服务器软件再通过另一块网卡与内部网络相连接。也就是说，外部网络与内部网络不能直接通信，它们之间的通信必须经过双宿主主机的过滤和控制，如图5.14所示。

这种配置是用双宿主主机做防火墙，两块网卡各自在主机上运行着防火墙软件，可以

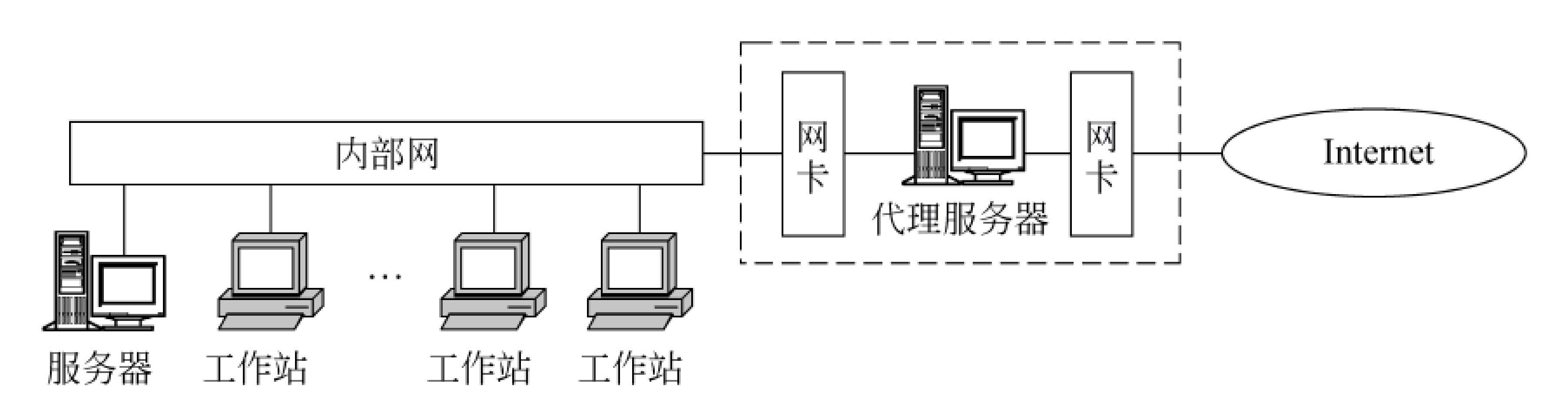


图 5.14 双宿主主机网关

转发应用程序、提供服务等。应该指出的是，在建立双宿主主机时，应该关闭操作系统的路由能力，否则从一块网卡到另一块网卡的通信会绕过代理服务器软件，而使双宿主主机网关失去“防火”的作用。

这种配置的优点是：网关可将受保护网络与外界完全隔离；代理服务器可提供日志，有助于网络管理员确认哪些主机可能已被入侵；同时，由于它本身是一台主机，所以可用于诸如身份验证服务器及代理服务器，使其具有多种功能。它的缺点是：双宿主主机的每项服务必须使用专门设计的代理服务器，即使较新的代理服务器能处理几种服务，也不能同时进行；另外，一旦双宿主主机受到攻击，并使其只具有路由功能，那么任何网上用户都可以随便访问内部网络了，这将严重损害网络的安全性。

3. 屏蔽主机网关

屏蔽主机网关由屏蔽路由器和应用网关组成，屏蔽路由器的作用是包过滤，应用网关的作用是代理服务。这样，在内部网络和外部网络之间建立了两道安全屏障，既实现了网络层安全，又实现了应用层安全。来自外部网络的所有通信都会连接到屏蔽路由器，它根据所设置的规则过滤这些通信。在多数情况下，与应用网关之外的机器的通信都会被拒绝。网关的代理服务器软件用自己的规则，将被允许的通信传送到受保护的网络上。在这种情况下，应用网关只有一块网卡，因此它不是双宿主主机网关，如图 5.15 所示。

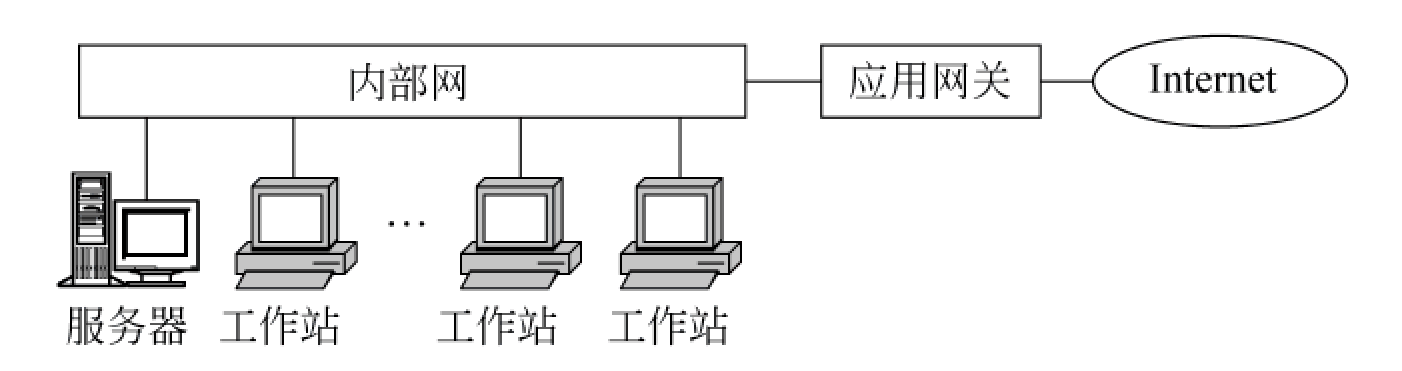


图 5.15 屏蔽主机网关

屏蔽主机网关比双宿主主机网关设置更加灵活，它可以设置成使屏蔽路由器将某些通信直接传到内部网络的站点，而不是传到应用层网关。另外，屏蔽主机网关具有双重保护，安全性更高。它的缺点是：由于要求对两个部件配置，使它们能协同工作，所以屏蔽主机的主机将失去任何安全保护，整个网络将对攻击者敞开。

4. 屏蔽子网

屏蔽子网系统结构是在屏蔽主机网关的基础上再加上一个屏蔽路由器，两个路由器

放在子网的两端，三者形成了一个被称为“非军事区”的子网，如图 5.16 所示。

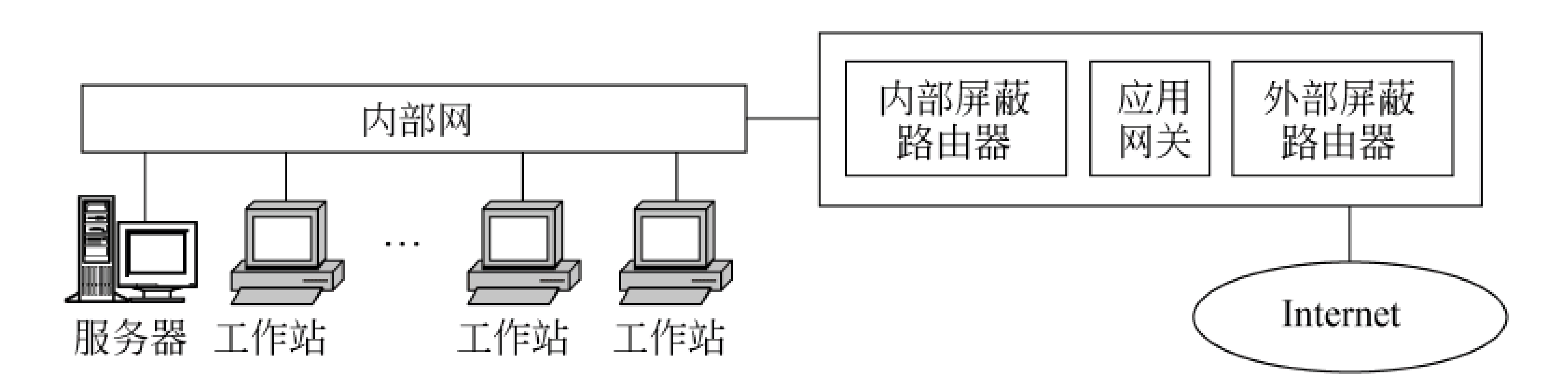


图 5.16　屏蔽子网

这种方法在内部网络和外部网络之间建立了一个被隔离的子网。用两台屏蔽路由器将这一子网分别与内部网络和外部网络分开。内部网络和外部网络均可访问被屏蔽子网，但禁止它们穿过被屏蔽子网通信。外部屏蔽路由器和应用网关与在屏蔽主机网关中的功能相同，内部屏蔽路由器在应用网关和受保护网络之间提供附加保护。为了入侵用这种体系结构构筑的内部网络，攻击者必须通过两个路由器。即使攻击者成功侵入了应用网关，他仍将面对内部路由器，这就消除了内部网络的单一入侵点。在屏蔽子网防火墙系统结构中，应用网关和屏蔽路由器共同构成了整个防火墙的安全基础。

屏蔽子网防火墙系统结构的不足之处是：它要求的设备和软件模块是上述几种防火墙系统结构最多的，其配置也相当复杂和昂贵。

5.4　常见的防火墙软件

防火墙是网络安全中重要的第一防线，越来越多的人认识到安装防火墙的重要性。下面介绍几个防火墙产品，这些厂家都获得了国际计算机安全协会的认证资格，所以不需要测试网络抵御攻击的能力。

1. Check Point Firewall-1

Check Point(www.checkpoint.com)公司推出的 Firewall-1 共支持两个平台：一个是 UNIX 平台；另一个是 Windows NT 平台。Firewall-1 具有一种很特别的结构，称为多层次状态监视结构。这种结构让 Firewall-1 可以对复杂的网络应用软件进行快速支持。也因为这个功能，使 Check Point 也提供了一套 APL 供开发者使用，以便开发更多的辅助工具。

Firewall-1 提供了最佳权限控制、最佳综合性能及简单明了的管理。除了 NAT 外，它具有用户认证功能。对于 FTP，可以根据 put、set 及文件名加以限制。对于 SMTP，它可以丢弃超过一定大小的邮件，对邮件进行病毒扫描，以及改写邮件头信息。Firewall-1 还可以防止有害 SMTP 命令(如 Debug)的执行。

Firewall-1 的用户界面是网络控制中心，定义和实施复杂的安全规则非常容易。每个规则还有一个域用于文档记录，如为什么制定这条规则，何时制定及由谁制定。

2. AXENT Raptor

Raptor 是代理型防火墙中最好的。它的界面易读、易操作，在实时日志方面，仅次于 Firewall-1。Raptor 的优势还在于其代理的深度和广度，只有它提供对 Microsoft NT 服务器的保护。它还具有 SQL * NET 代理功能，可控制对 Oracle 数据库的访问。Raptor 在 SMTP 方面做得很好，而且它是唯一可防止缓存溢出的防火墙，它可以代理 NNTP(网络新闻协议)和 NTP(网络时间协议)。

3. 天网防火墙个人版

天网防火墙个人版是个人计算机使用的网络安全程序，根据管理者设定的安全规则把守网络，提供强大的访问控制、信息过滤等功能，帮你抵挡网络入侵和攻击，防止信息泄露。天网防火墙把网络分为本地网和 Internet，可针对来自不同网络的信息，来设置不同的安全方案，适合于任何方式上网的用户。

(1) 严密的实时监控

天网防火墙(个人版)对所有来自外部机器的访问请求进行过滤，发现非授权的访问请求后立即拒绝，随时保护用户系统的信息安全。

(2) 灵活的安全规则

天网防火墙(个人版)设置了一系列安全规则，允许特定主机的相应服务，拒绝其他主机的访问要求。用户还可以根据自己的实际情况，添加、删除、修改安全规则，保护本机安全。

(3) 应用程序规则设置

新版的天网防火墙增加对应用程序数据包进行底层分析拦截功能，它可以控制应用程序发送和接收数据包的类型、通信端口，并且决定拦截还是通过，这是目前其他很多软件防火墙不具有的功能。

(4) 详细的访问记录和完善的报警系统

天网防火墙(个人版)可显示所有被拦截的访问记录，包括访问的时间、来源、类型、代码等都详细地记录下来，你可以清楚地看到是否有入侵者想连接到你的机器，从而制定更有效的防护规则。与以往的版本相比，天网防火墙(个人版)设置了完善的声音报警系统，当出现异常情况的时候，系统会发出预警信号，从而让用户做好防御措施。



【案例】 应用天网防火墙防范木马

操作步骤

在全面了解天网防火墙的设置之后，再来讲述一下其防范木马的主要方法。对于木马程序第一次运行的情况，可采用如下防御方法。

第 1 步 如果在天网防火墙运行时，木马服务器程序要打开网络端口，此时会弹出“天网防火墙警告信息”对话框，即可很容易检测到自己运行的程序是否被绑定了木马。

第 2 步 如果要想防止某程序使用网络资源，则单击“天网防火墙警告信息”信息提

示框中的“禁止”按钮即可，这样，攻击者就无法通过木马服务器程序来对被攻击者的机器进行远程控制了。而对于那些已经被植入木马到计算机中的用户，则可以采用如下的防御方法。

第 3 步　在天网防火墙主窗口中单击“增加规则”按钮，即可打开“增加 IP 规则”对话框，在“规则”选项组的“名称”文本框中输入“禁止冰河木马的入侵”，在“说明”文本框中输入“记录冰河木马入侵，方法是记录 7626 端口的访问情况，在发现有冰河木马入侵的时候，同时发声”。在“数据包方向”下拉列表中选择“接收”选项，再在“对方 IP 地址”下拉列表中选择“任何地址”选项，如图 5.17 所示。

第 4 步　在“数据包协议类型”下拉列表中选择“TCP”选项之后，即可出现 TCP 类型框，在“本地端口”选项组中设定端口为从 7626 到 7626，如图 5.18 所示。在“数据包协议类型”下拉列表中选择 UDP 项之后，将出现 UDP 类型框，如图 5.19 所示，在“本地端口”选项组中设定端口为从 7626 到 7626。

这两处(TCP/UDP)的设置主要是为了监听 7626 端口而进行的，因为冰河木马服务器程序就是使用这个端口与客户端程序进行通信的。

第 5 步　在“当满足上面条件时”下拉列表中选择“通行”选项之后，再在“同时还”选项组中选中“记录”和“发声”复选框，如图 5.20 所示。此时，在自定义 IP 规则列表框中就可以看到已经出现“禁止冰河木马的入侵”规则了，如图 5.21 所示。

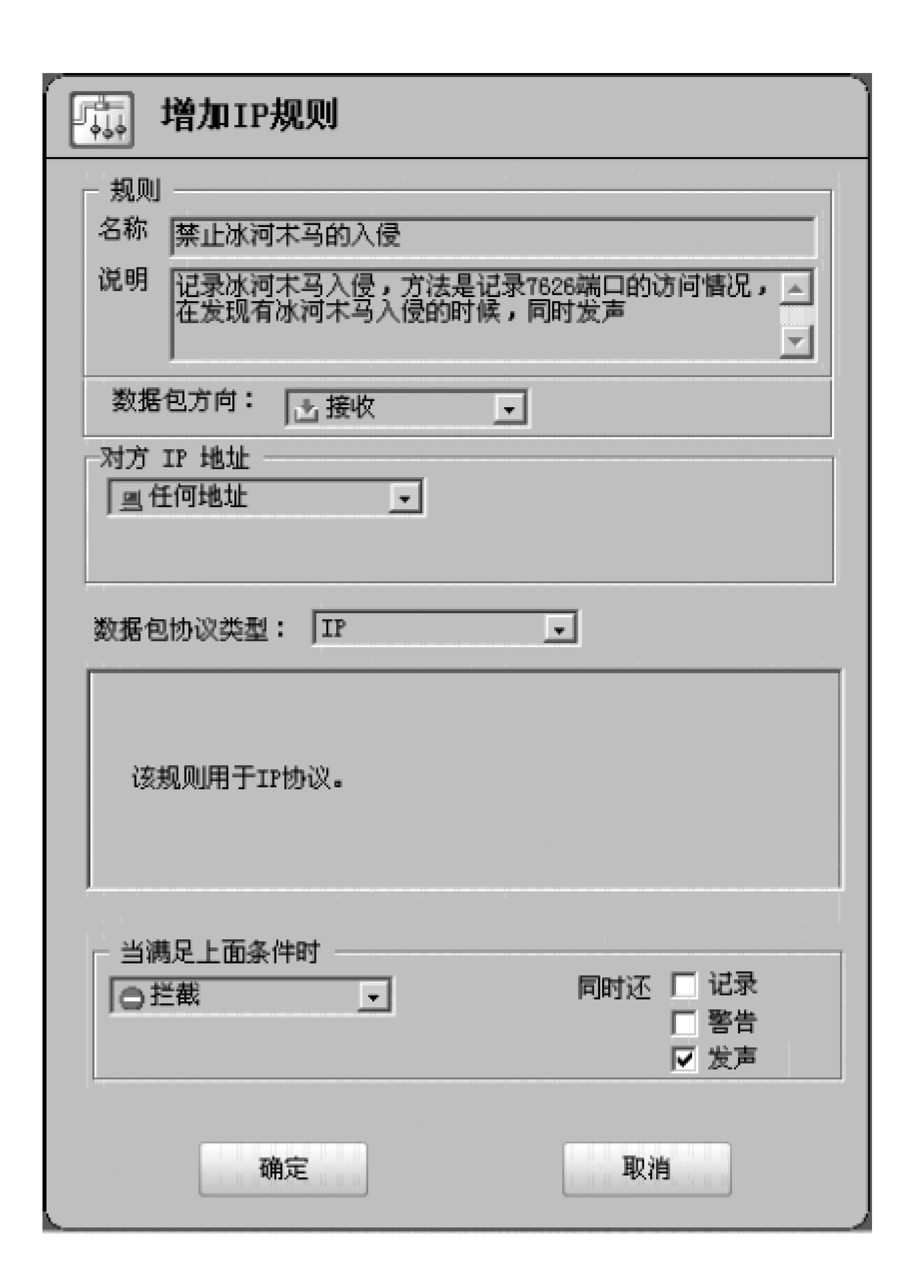


图 5.17　设置数据包方向和对方 IP 地址



图 5.18　TCP 类型

图 5.19　UDP 类型

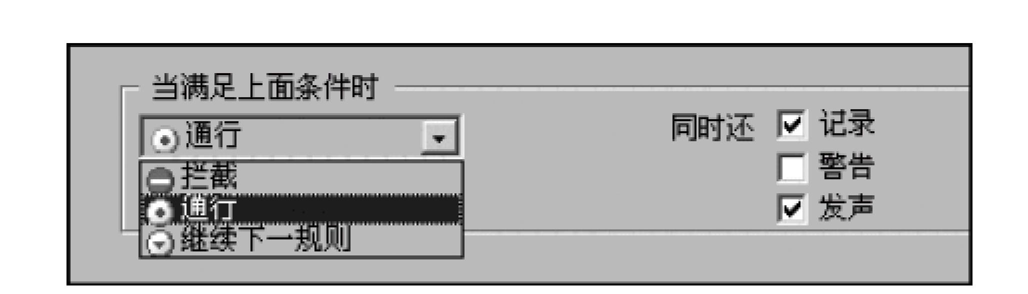


图 5.20　设置动作

经过上述设置之后，只要有其他计算机想通过冰河客户端程序控制本地计算机，本地计算机可出现“!”在“天网防火墙”图标上下不断闪烁，并同时还发出警报声音。单击“日志”按钮之后，天网防火墙可显示是哪些 IP 通过木马访问本地计算机的提示信息。



图 5.21　出现“记录冰河入侵”规则

【案例】 天网防火墙在端口上的应用

1. 应用天网防火墙开放 BT 端口

案例分析

BT 使用的端口为 6881～6889 端口这 9 个端口，而防火墙的默认设置是不允许访问这些端口的，它只允许 BT 软件访问网络，所以有时在一定程度上影响了 BT 下载速度。下面应用无网防火墙开放 6881～6889 端口。

操作步骤

第 1 步　在天网防火墙主窗口中单击“增加规则”按钮后，按照如图 5.22 所示进行设置。单击“确定”按钮完成新规则的建立，将新规则命名为 BT。

第 2 步　保存设置的新规则，然后进行在线端口测试 BT 的连接端口是否已经开放的。



图 5.22　修改 IP 规则

2. 打开 21 和 80 端口

案例分析

很多人都使用了 FTP 服务器软件和 Web

服务器,防火墙不仅限制本机访问外部的服务器,也限制外部计算机访问本机。为了Web和FTP服务器能正常使用,我们就必须设置防火墙。

操作步骤

第1步 按图5.23所示设置打开Web服务80端口的IP规则。

第2步 单击“确定”按钮,并使其生效。

第3步 按图5.24所示设置打开FTP服务21端口的IP规则。

第4步 单击“确定”按钮使设置生效。

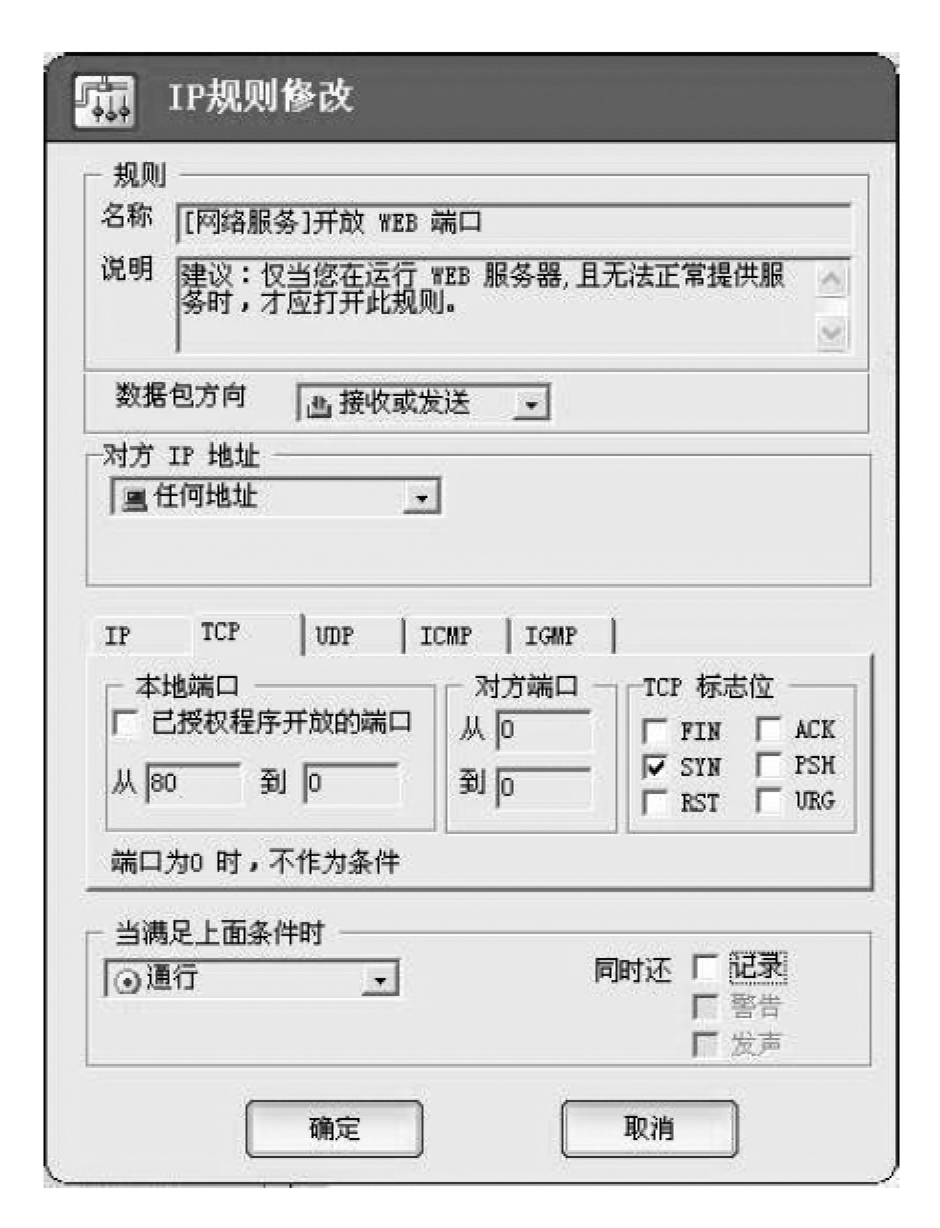


图5.23 “IP规则修改”对话框

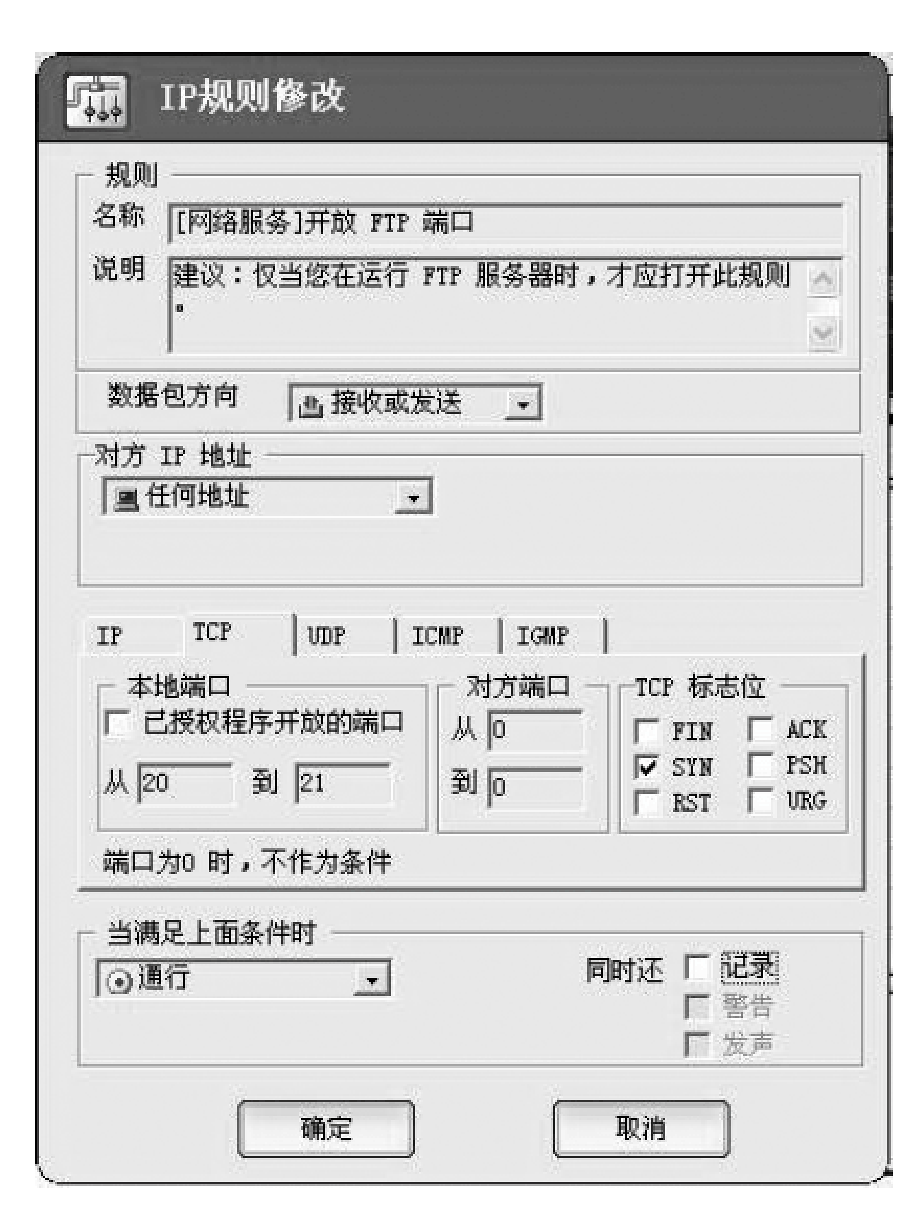


图5.24 打开FTP服务21端口的IP规则

5.5 防火墙选购策略

选用防火墙首先要明确哪些数据是必须保护的,这些数据被侵入会导致什么样的后果及网络不同区域需要什么等级的安全级别,因此,首先要根据信息系统安全级别确定。其次才是防火墙的功能,选用防火墙必须与网络接口匹配,要防止你所能想到的威胁,防火墙可以是软件或硬件模块,并能集成于网桥、网关、路由器等设备之中。选用防火墙的原则主要有以下几点。

1. 防火墙自身的安全性

大多数人在选择防火墙时都将注意力放在防火墙如何控制连接及防火墙支持多少种服务上,但往往忽略一点,防火墙也是网络上的主机设备,也可能存在安全问题。防火墙如果不能确保自身安全,则防火墙的控制功能再强也终究不能安全保护内部网络。

通常防火墙都安装在一般的操作系统(如 UNIX、Windows 2000 等)上。在防火墙主机上执行的除了防火墙软件外,程序、系统核心也大多来自操作系统本身的原有程序。当防火墙上所执行的软件出现安全漏洞时,防火墙本身也将受到威胁。此时,任何的防火墙控制机制都可能失效。因为当一个黑客取得了防火墙上的控制权以后,黑客几乎可以为所欲为地修改防火墙上的存取规则,进而侵入更多的系统。因此,防火墙自身仍应有相当高的安全保护。

2. 应考虑的特殊需求

企业安全策略中往往有些特殊需求,不是每一个防火墙都会提供的,这是选择防火墙需考虑的因素之一,常见的需求如下。

(1) IP 转换

进行 IP 转换有两个好处:其一是隐藏内部网络真正的 IP,这可以使黑客无法直接攻击内部网络,也是要强调防火墙自身安全性问题的主要原因;其二是可以让内部网络保留 IP,这对许多 IP 不足的企业是有益的。

(2) 双重 DNS

当内部网络使用没有注册的 IP 地址或是防火墙进行 IP 转换时,DNS 也必须经过转换。因为,同样的一个主机在内部的 IP 与给予外界的 IP 将会不同,有的防火墙会提供双重 DNS,有的则必须在不同主机上各安装一个 DNS。

(3) 虚拟专用网络

虚拟专用网络(VPN)可以在防火墙与防火墙或移动的客户机间对所有网络传输的内容加密,建立一个虚拟通道,让两者间感觉是在同一个网络上,可以安全且不受拘束地互相存取,这对总公司与分公司之间或公司与外出的员工之间,需要直接联系又不愿花费大量金钱,在申请专线或用长途电话拨号连接时,将会非常有用。

(4) 扫毒功能

大部分防火墙都可以与防病毒防火墙搭配实现扫毒功能。有的防火墙则可以直接集成扫毒功能,差别只是扫毒工作是由防火墙完成,或是由另一台专用的计算机完成。

(5) 特殊控制需求

有时候企业会有特别的控制需求,如限制特定使用者才能发送电子邮件,FTP 只能 GET 档案不能 PUT 档案,限制同时上网人数,还有使用时间或 Block Java、ActiveX 等,依需求不同而定。

3. 防火墙系统的稳定性和可靠性

就一个成熟的产品来说,保障系统的稳定性是最基本的要求。目前,由于种种原因,国内有些防火墙尚未最后定型或没有经过严格的、大量的测试就被推向了市场,这样一来,其稳定性就可想而知了。防火墙的稳定性情况从厂家的宣传材料中是看不出来的,但可以从一些渠道获得,如国家权威的测评认证机构、对产品的咨询、调查及试用、厂商开发研制的历史及实力等方面。

可靠性对防火墙设备来说尤为重要,其直接影响受控制网络的可用性。提高可靠性

的措施一般是提高本身部件的健壮性、增大设计阈值和增加冗余部件，这要求有较高的生产标准和设计冗余度，如使用工业标准、电源热备份、系统热备份等。

4. 防火墙的性能

高性能是防火墙的一个重要指标，它直接体现了防火墙的可用性，也体现了用户使用防火墙所需付出的安全代价。如果由于使用防火墙而带来了网络性能较大幅度下降，就意味着安全代价过高，用户是无法接受的。一般来说，防火墙加载上百条规则后，其性能下降不应超过5%。

对通信行为的有效控制，要求防火墙设备有一系列不同级别，以满足不同用户的各类安全控制需求。防火墙控制的有效性、多样性、级别目标的清晰性、制定的难易性和经济性等，体现着防火墙的高效和质量。如对普通用户，只要对IP地址进行过滤即可；如果是内部有不同安全级别的子网，有时则必须允许高级别子网对低级别子网进行单向访问；如果还有移动用户的话，还要求能根据用户身份进行过滤。

防火墙过滤报文时，最基础的是针对IP地址进行过滤。而IP地址是非常容易修改的，只要打听到内部网里谁可以穿过防火墙，那么将自己的IP地址改成与他的一样就可以了。这就需要一个针对用户身份而不是IP地址进行过滤的办法。目前防火墙上常用的一次性口令验证机制，通过特殊的算法，保证用户在登录防火墙时，口令不会在网络上泄露，这样，防火墙就可以确认登录上来的用户确实与他所声称的一致。

用户的网络不是一成不变的，防火墙现在可能主要是在内部网和外部网之间进行过滤，随着网络的发展，内部网络可能出现具有不同安全级别的子网，这时就需要在子网之间过滤。因此，在购买防火墙时必须清楚，是否可以增加网络接口，是否具有扩展性。

随着网络技术的发展和黑客攻击手段的不断变化，防火墙也必须不断地进行升级，此时支持软件升级就很重要了。如果不支持软件升级的话，为了抵御新的攻击手段，用户就必须进行硬件上的更换，而在更换期间用户的网络是不设防的，同时也要为此花费更多的钱。

5. 防火墙配置的方便性

在网络入口和出口处安装新的网络设备是比较复杂的，这意味着必须修改几乎所有现有设备的配置，因此，应选用方便配置的、支持透明通信的防火墙。它在安装时不需要对原网络配置做任何改动，所做的工作只相当于连接一个网桥或HUB。需要时，两端连线就可以工作，不需要时，将网线恢复原状即可。

防火墙的管理在充分考虑安全需要的前提下，必须提供更方便、灵活的管理方式和方法。通常体现为管理途径、管理工具和管理权限。防火墙设备首先是一个网络通信设备，管理途径的提供要兼顾通常网络设备的管理方式。管理工具主要为GUI类管理器，用它管理很直观，这对于设备的初期管理和不太熟悉的管理人员来说是一种有效的管理方式。权限管理是管理本身的基础，但是，应防止严格的权限认证可能带来的管理方便性的降低。

以上就是选购防火墙时需要注意的一些问题，同时要明白，没有一种技术可以百分之

百地解决网络上的所有问题。网络安全会受到许多因素的影响，诸如安全策略、职员的技术背景、费用及估计可能受到的攻击等。只有正确地认识防火墙，并合理使用，才是最安全的。

本章小结

防火墙是用于保护计算机网络中敏感数据不被窃取和篡改的计算机软硬件系统。

防火墙技术分为包过滤防火墙技术和代理防火墙技术。

防火墙体系应该是多种解决不同问题的技术的有机组合。常见的配置有屏蔽路由器、双宿主主机网关、屏蔽主机网关、屏蔽子网等几种。

防火墙在选购时应注意策略，如何选购一个安全、稳定、可靠的防火墙产品是非常重要的。

防火墙是目前用来实现网络安全措施的一种主要手段。

本章练习

一、填空题

1. 常用的防火墙可以分为________和________两大类。
2. 代理防火墙作用________层。
3. 双宿主主机网关中的双宿主主机是一台安装有________的计算机。
4. 屏蔽主机网关由________和________组成。
5. 屏蔽子网系统结构是在________基础上再加上一个屏蔽路由器构成。

二、选择题

1. 防火墙自身有一些限制，它不能阻止________威胁。

 Ⅰ. 外部攻击　　Ⅱ. 内部攻击　　Ⅲ. 病毒感染

 A. Ⅰ　　B. Ⅰ和Ⅱ　　C. Ⅱ和Ⅲ　　D. 全部

2. 关于防火墙，以下说法错误的是________。

 A. 防火墙能隐藏内部 IP 地址

 B. 防火墙能控制进出内网的信息流向和信息包

 C. 防火墙能提供 VPN 功能

 D. 防火墙能阻止来自内部的威胁

3. ________技术不是实现防火墙的主流技术。

 A. 包过滤技术　　B. 应用级网关技术

 C. 代理服务器技术　　D. NAT 技术

4. 目前，防火墙一般可以提供 4 种服务，它们是________。

 A. 服务控制、方向控制、目录控制和行为控制

B. 服务控制、网络控制、目录控制和方向控制
C. 方向控制、行为控制、用户控制和网络控制
D. 服务控制、方向控制、用户控制和行为控制

5. 防火墙采用的最简单的技术是________。
A. 安装保护卡　B. 隔离　C. 包过滤　D. 设置进入密码

三、简答题

1. 什么是防火墙？防火墙分为哪几类？
2. 防火墙有哪些功能特点？
3. 试述包过滤防火墙技术的原理及特点。
4. 试述代理防火墙技术的原理及特点。
5. 常见的防火墙体系结构有哪几种？
6. 选购防火墙应注意哪些？

实训　使用瑞星防火墙防御网络攻击

实训目的

（1）了解防火墙系统的基本原理。
（2）掌握瑞星防火墙的使用方法。

实训环境

（1）连上 Internet 的主机或局域网主机。
（2）Windows XP/2003 系统。
（3）瑞星防火墙 2012 个人版。

实训步骤

第 1 步　认识瑞星防火墙软件后，选择“开始”→“所有程序”→“瑞星防火墙”命令即可启动瑞星防火墙，其主界面如图 5.25 所示。

第 2 步　设置防火墙常规选项。

（1）网络防护设置

启动防火墙主程序，单击“设置”按钮，进入“设置”窗口，选择“网络防护”选项，如图 5.26 所示，可以进行以下设置。

① 程序联网控制。
② 网络攻击拦截。
③ 恶意网址拦截。
④ ARP 欺骗防御。
⑤ 对外攻击拦截。



图 5.25　瑞星个人防火墙主界面



图 5.26　“网络防护”界面

⑥ 网络数据保护。

⑦ IP 规则设置。

(2) 升级设置

单击“设置”按钮，进入设置界面，选择“升级设置”选项，进入图 5.27 所示的“升级设置”界面，可以进行以下设置。

① 使用 Internet Explorer 的设置连接网络。



图 5.27 “升级设置”界面

② 通过局域网或直接连接访问网络。

③ 通过代理服务器访问网络。

(3) 高级设置

单击“设置”按钮，进入设置界面，选择“高级设置”选项，进入图 5.28 所示的“高级设置”界面，可以进行以下设置。



图 5.28 “高级设置”界面

① 软件安全。

② “云安全”计划。

第 3 步　首页网络安全监控。进入图 5.29 所示的“首页”选项卡。在该界面下，可以对防火墙工作情况进行监控。



图 5.29　“首页”界面

第 4 步　设置网络防护。选择“网络防护”选项卡，进入图 5.30 所示的“网络防护”界面。在此处对网络防护的状态及具体内容进行设置。



图 5.30　“网络防护”界面

第 5 步　联网程序监控。选择“联网程序”选项卡，进入图 5.31 所示的“联网程序”界

面，在此对联网程序的状态进行监控。



图 5.31 “联网程序”界面

第 6 章

入侵检测技术

Chapter 6

知识目标

- 掌握入侵检测的概念、功能特点和安全性。
- 了解入侵检测系统的分类。
- 了解常用的入侵检测系统产品。

技能目标

- 能使用常用的入侵检测系统。
- 能选购、安装和维护入侵检测系统。

6.1 入侵检测技术简介

1. 什么是入侵检测系统

入侵检测系统(intrusion detection system,IDS)是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的系统,是一种用于检测计算机网络中违反安全策略行为的系统。入侵和滥用都是违反安全策略的行为。

假如防火墙是一幢大楼的门锁,那 IDS 就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼,或内部人员有越界行为,只有实时监视系统才能发现情况并发出警告。入侵检测系统能够识别出任何不希望有的活动,这种活动可能来自于网络外部和内部。入侵检测系统的应用,能使在入侵攻击对系统发生危害前检测到入侵攻击,并利用报警与防护系统驱逐入侵攻击。在入侵攻击的过程中,能减少入侵攻击所造成的损失。在被入侵攻击后,收集入侵攻击的相关信息,作为防范系统的知识,添加到知识库内,以增强系统的防范能力。

入侵检测系统处于防火墙之后对网络活动进行实时检测。在许多情况下,由于可以记录和禁止网络活动,所以入侵检测系统是防火墙的延续。它们可以与防火墙和路由器配合工作。应当理解入侵检测系统是独立于防火墙工作的。

入侵检测系统与系统扫描器(system scanner)不同。系统扫描器是根据攻击特征数据库来扫描系统漏洞的,它更关注配置上的漏洞而不是当前进出主机的流量。在遭受攻击的主机上,即使正在运行扫描程序,也无法识别这种攻击。

入侵检测系统扫描当前网络的活动，监视和记录网络的流量，根据定义好的规则来过滤从主机网卡到网线上的流量，提供实时报警。网络扫描器检测主机上先前设置的漏洞，而 IDS 监视和记录网络流量。如果在同一台主机上运行 IDS 和扫描器的话，配置合理的 IDS 会发出许多报警。

2. 入侵检测的功能

(1) 监视分析用户和系统的行为。
(2) 审计系统配置和漏洞。
(3) 识别攻击行为。
(4) 评估敏感系统和数据的完整性。
(5) 对异常行为进行统计。
(6) 安装诱骗服务器，记录非法入侵行为。
(7) 进行审计跟踪，识别违反安全法规的行为。

3. 入侵检测系统的需求特性

(1) 可靠性。检测系统必须在无人监控的情况下连续运行。系统必须是可靠的，这样才可以允许它运行在被检测的系统环境中。
(2) 适应性。检测系统必须能随时追踪系统环境的改变。
(3) 有效性。能检测系统的报告错误或漏报控制在一定的范围内。
(4) 安全性。检测系统必须难于被欺骗，能够保护自身的安全。
(5) 容错性。检测系统的容错要求即使在系统崩溃的情况下，检测系统仍能保留下来。

4. 入侵检测的发展

入侵检测系统需要实现的目标是发现网络上所有的异常行为与错误，20 年来，入侵检测系统都是围绕着这个观念来发展的。但最近，对入侵检测系统的观点有了较大的转变，入侵检测系统逐渐普及并结合到其他的信息系统安全的各部分中。

入侵检测系统的概念诞生于 1980 年，James Anderson 发表了文章 *Computer Security Threat Monitoring and Surveillance*，这篇文章介绍了对网络上用户的行为及信息进行审计的一种方法。随着文章的发表，“检测”这个概念逐渐被用户所接受。Anderson 对于入侵检测的理论成为入侵检测系统设计及开发的基础，他的工作成为基于主机的入侵检测系统和其他入侵检测系统的出发点。

在 1983 年，SRI 组织和 Dorothy 博士开始了为一个政府项目而工作，将一些新的技术应用到入侵检测系统的开发当中。他们的目标是利用政府的大型计算机对用户的行为踪迹进行分析，然后在分析结果的基础上以建立用户的行为的轮廓模型。一年之后，Dorothy 博士帮助建立起了第一个入侵检测的模型：入侵检测专家系统(intrusion detection expert system，IDES)。这项工作为入侵检测技术的发展提供了良好的基础并带动了入侵检测基础的发展。

1984 年，SRI 开发了一种方法来跟踪和分析包含 ARPANET 用户身份验证信息的审计数据。很快，SRI 在与海军的一份合同中首次实现了入侵检测系统。入侵检测专家系统使用的是 Dorothy 博士在 SRI 工作期间的研究成果。Dorothy 博士发表的这个有决定性的成果，一个入侵检测系统模型，为开发商业化入侵检测系统提供了必不可少的信息，她的文章成为入侵检测系统发展的基础。

1988 年，在美国空军一个名为"干草堆"的项目中，另一种版本的入侵检测系统也被实现了。这个项目的产品是一个通过分析审计数据并与比较其中是否存在已定义的内容来工作的入侵检测系统。一位前"干草堆"项目的成员说："在一大堆数据中查找是否有特点细节的行为就如同在干草堆中寻找一根针。"

在这之后，通过在网络中同时布置多个入侵检测系统协同工作的方式也诞生了，这种方式被称为分布式入侵检测系统(distributed intrusion detection system，DIDS)。分布式入侵检测系统是原有入侵检测系统的扩展，这样通过跟踪客户机的方式比原来监视服务器的方式要好得多。最后，在 1989 年，"干草堆"项目发展形成了一个商业公司，"干草堆"实验室同时发布使用新一代技术的产品 Stalker，Stalker 是一个基于网络的入侵检测系统。

进入 20 世纪 90 年代后，网络入侵检测系统的概念被提出。1990 年，Heberlein 作为最主要的开发者开发出了网络安全监视器(network security monitor，NSM)，这就是第一个网络入侵检测系统。这种新的方式引起了入侵检测行业及风险投资的极大兴趣。Heberlein 的贡献甚至影响到了分布式入侵检测系统项目发展方向，加入"干草堆"开发小组，他提出了第一个混合入侵检测系统的想法，他介绍的网络入侵检测系统引起入侵检测行业的一次革命，并将"干草堆"项目带往商业道路上。

入侵检测技术的商业化最早是在 1990 年年初，"干草堆"实验室第一个推出一个商业化的入侵检测工具 Stalker。Stalker 是一个标准的基于主机的入侵检测系统，而正在开发的 SAIC 则是另一种形式的入侵检测系统，称为计算机错误检测系统(computer misuse detection system，CMDS)。同时，美国空军的密码技术中心也开发出一种审计安全衡量系统(audit security measurement system，ASIM)，用于监视美国空军网络传输数据。与其他的网络入侵检测系统相比，审计安全衡量系统的优势在于可量测性和便于携带。审计安全衡量系统也是第一个将硬件与软件结合的网络入侵检测解决方案。审计安全衡量系统被美国空军计算机安全紧急响应中心广泛应用在全世界各地。ASIM 项目的开发小组在 1994 年也发展成了一家商业公司 the Wheel Group，他们的产品 NetRanger，是第一个可用于商业化的网络入侵检测系统。

入侵检测市场逐渐扩大并开始带来收入是在 1997 年左右，在这一年，Cisco 公司认识到网络入侵检测的重要性并收购了 the Wheel Group，并开始向客户提供安全解决方案。同样，网络安全行业的领导者，ISS 公司也开发出了自己的网络入侵检测系统 RealSecure。一年后，第一个可视化基于主机入侵检测系统的公司(Centrax 的公司)与"干草堆"实验室合并。从此，入侵检测的世界逐渐为市场所主导。

由于入侵检测系统的市场在近几年中飞速发展，许多公司投入到这一领域上来。除了国外的 ISS、Axent、NFR、Cisco 等公司外，国内也有数家公司(如中联绿盟、中科网威

等)推出了自己相应的产品。但就目前而言,入侵检测系统还缺乏相应的标准。有两个组织试图对IDS进行标准化工作:IETF的IDWG(intrusion detection working group)和CIDF(common intrusion detection framework),但其工作进展非常缓慢,尚没有被广泛接受的标准出台。

6.2 入侵检测系统的组成

6.2.1 入侵检测系统的组成

从功能上讲,入侵检测系统由探测器(sensor)、分析器(analyzer)和用户接口(user interface)组成。下面分别对这3个部分进行简要介绍。

1. 探测器

探测器主要负责收集数据。探测器的输入数据包括任何可能包含入侵行为线索的数据,如网络数据包、日志文件和系统调用记录等。探测器将这些数据收集起来,然后发送到分析器进行处理。

2. 分析器

分析器又可称为检测引擎(detection engine),它负责从一个或多个探测器处接收信息,并通过分析来确定是否发生了非法入侵活动。分析器组件的输出是标识入侵行为是否发生的指示信号,如一个警告信号,该指示信号中还可能包括相关的证据信息。另外,分析器组件还能够提供关于可能反应措施的信息。

3. 用户接口

IDS的用户接口使得用户易于观察系统的输出信息,并对系统行为进行控制。在某些系统中,用户接口又可称为“管理器”、“控制器”或者“控制台”等。

除了以上3个必要组件之外,某些IDS可能还包括一个所谓的“蜜罐”(honeypot)诱饵机。该诱饵机被设计和配置成为具有明显的系统安全漏洞,并对攻击者明显可见。诱饵机能够作为IDS中一个专门提供给攻击者进行入侵的探测器来使用,从而提供关于某次攻击行为的发生过程和相关信息。

6.2.2 入侵检测系统的类型

从技术上看,入侵检测系统可以分为基于主机的入侵检测系统、基于网络的入侵检测系统、混合入侵检测和网络节点的入侵检测等。

1. 基于主机的入侵检测

基于主机的入侵检测(host-based intrusion detection,HID)系统用于监视、检测对于主机的攻击行为,并通知用户并进行响应。有些功能强大的工具甚至能提供审计策略管

理与集中控制，提供数据对比、统计与分析支持。

基于主机的入侵检测设备通常是安装在被重点检测的主机之上，其目标主要是主机系统和本地用户，主要是对该主机的网络实时连接及系统审计日志进行智能分析和判断。如果其中主体活动十分可疑（特征或违反统计规律），入侵检测系统就会采取相应的措施。基于主机的入侵检测系统的结构如图6.1所示。

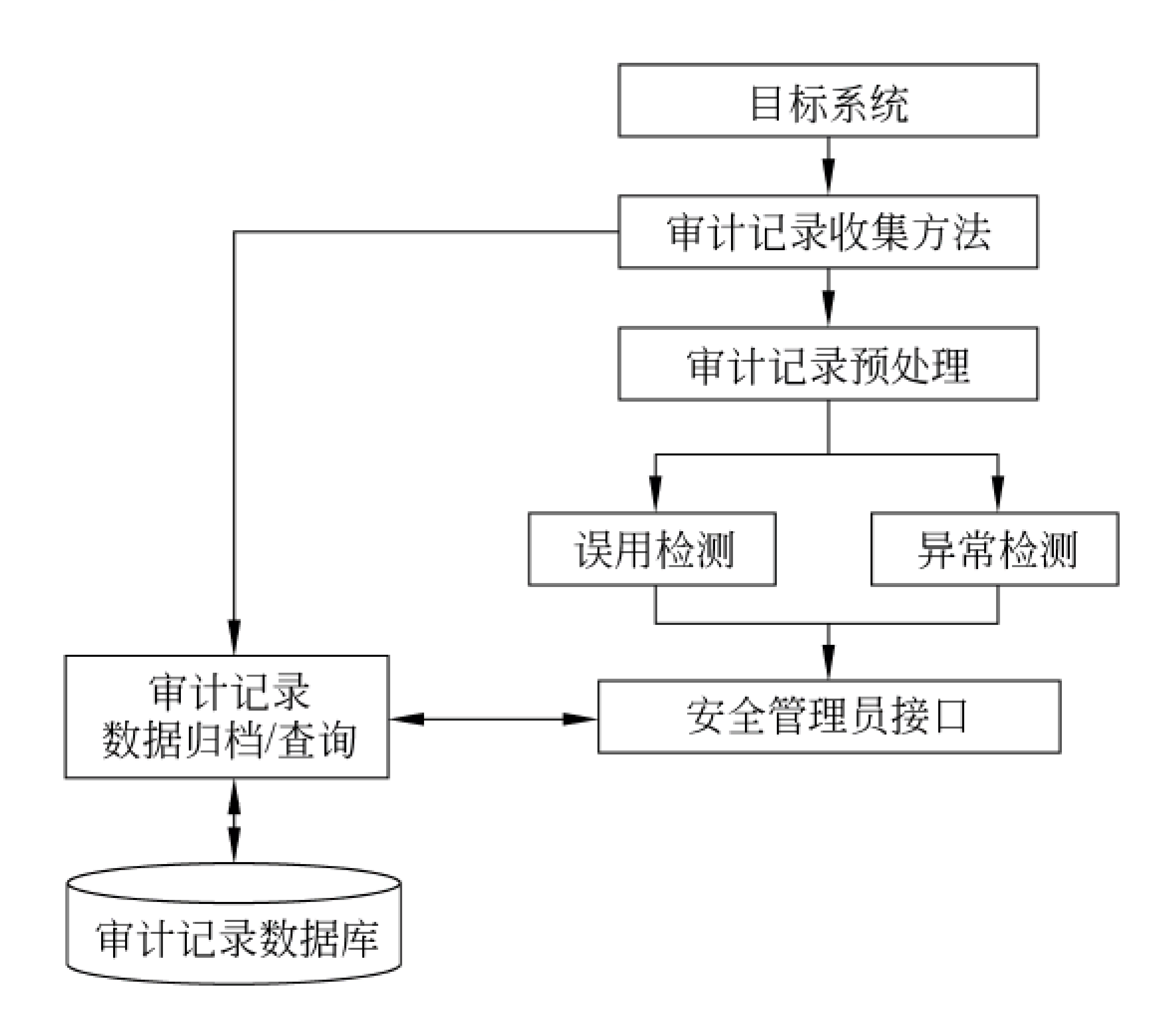


图6.1 基于主机的入侵检测系统

（1）基于主机的入侵检测系统对分析“可能的攻击行为”非常有用。举例来说，有时候它除了指出入侵者试图执行一些“危险的命令”之外，还能分辨入侵者干了什么事，他们运行了什么程序、打开了哪些文件、执行了哪些系统调用。基于主机的入侵检测系统与基于网络的入侵检测系统相比通常能够提供更详尽的相关信息。

（2）基于主机的入侵检测系统通常情况下比网络入侵检测系统误报率要低，因为检测在主机上运行的命令序列比检测网络流量更简单，系统的复杂性也少得多。

（3）基于主机的入侵检测系统可安装在那些不需要广泛的入侵检测、传感器与控制台之间的通信带宽不足的情况下。主机入侵检测系统在不使用诸如“停止服务”、“注销用户”等响应方法时风险较少。

基于主机的入侵检测系统的弱点如下。

（1）基于主机的入侵检测系统安装在我们需要保护的设备上。例如，当一个数据库服务需要保护时，就要在服务器本身安装入侵检测系统。这会降低应用系统的效率。

（2）基于主机的入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必须重新配置，这将会给运行中的业务系统带来不可预见的性能影响。

（3）全面安装基于主机的入侵检测系统代价较大，企业中很难将所有主机用主机入侵检测系统保护，只能选择分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器达到攻击目标。

（4）基于主机的入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。

对入侵行为分析的工作量将随着主机数目增加而增加。

2. 基于网络的入侵检测

基于网络的入侵检测(network intrusion detection,NID)是通过分析主机之间网络上传输的信息来工作的。网络入侵检测设备能截取利用不同传输介质及不同协议进行传输的数据包(大部分入侵检测系统主要是针对 TCP/IP 协议)。

基于网络的入侵检测设备(NIDS)放置在比较重要的网段内,不停地监视网段中的各种数据包。对每一个数据包或可疑的数据包进行特征分析。如果数据包与产品内置的某些规则吻合,入侵检测系统就会发出警报甚至直接切断网络连接。目前,大部分入侵检测产品是基于网络的。基于网络的入侵检测系统是根据网络流量、网络数据包和协议来分析检测入侵行为的。其基本过程如图 6.2 所示。

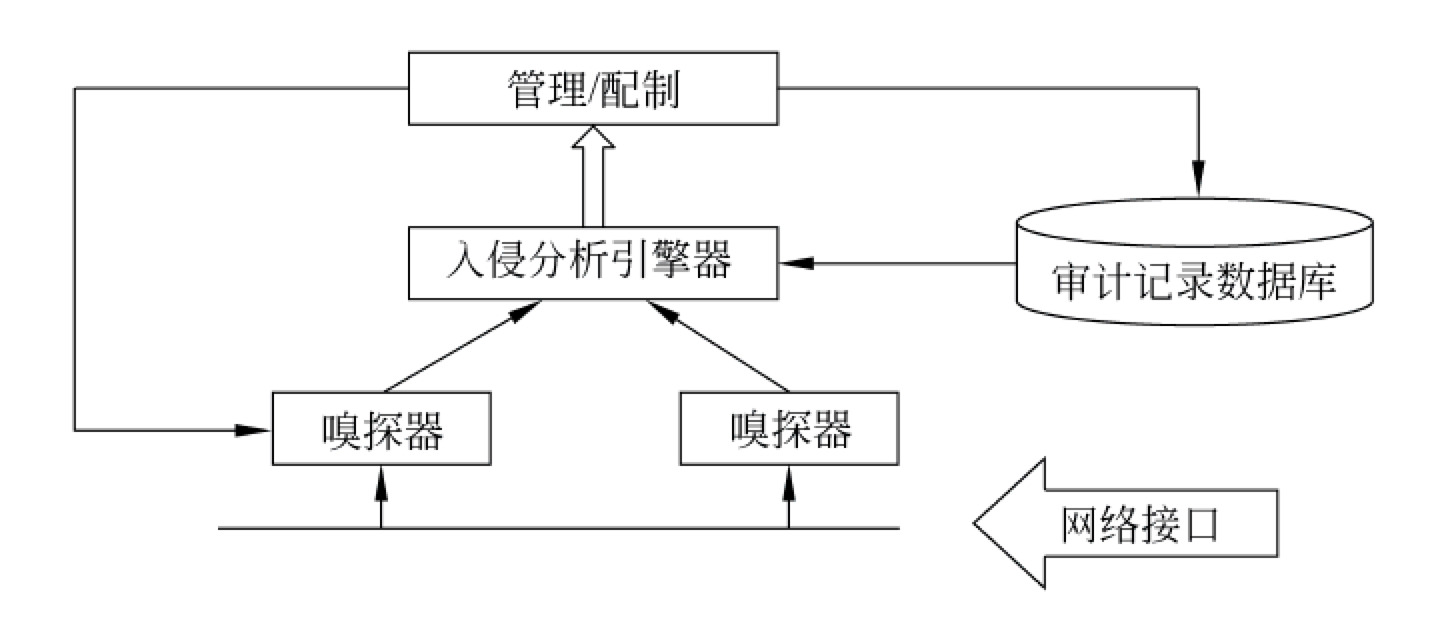


图 6.2　基于网络的入侵检测系统

基于网络的入侵检测系统的优点如下。

(1) 基于网络的入侵检测系统能够检测那些来自网络的攻击,它能够检测到超过授权的非法访问。

(2) 一个基于网络的入侵检测系统不需要改变服务器等主机的配置。由于它不会在业务系统的主机中安装额外的软件,从而不会影响这些机器的 CPU、I/O 与磁盘等资源的使用,不会影响业务系统的性能。

(3) 由于基于网络的入侵检测系统不像路由器、防火墙等关键设备那种方式工作,它不会成为系统中的关键路径。基于网络的入侵检测系统发生故障不会影响正常业务的运行。安装基于网络的入侵检测系统的风险比安装基于主机的入侵检测系统的风险小得多。

(4) 基于网络的入侵检测系统近几年有向专门设备发展的趋势,安装一个基于网络的入侵检测系统非常方便,只需将定制的设备接上电源,做很少的配置,将其连到网络上即可。

基于网络的入侵检测系统的弱点如下。

(1) 基于网络的入侵检测系统只检测它直接连接网段的通信,不能检测在不同网段的网络包。在使用交换以太网的环境中会出现检测范围的局限。而安装多台基于网络的入侵检测系统的传感器会使整个系统的成本大大增加。

(2) 基于网络的入侵检测系统为了性能目标通常采用特征检测的方法,它可以检测

出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

(3) 基于网络的入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样的系统中的传感器协同工作能力较弱。

(4) 基于网络的入侵检测系统处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着 IPv6 的普及，这个问题会越来越突出。

随着网络系统结构复杂化和大型化，出现了许多基于分布式的入侵检测，例如：

(1) 系统的弱点或漏洞分散在网络中各个主机上，这些弱点可能被入侵者一起用来攻击网络，而依靠唯一的主机或网络 IDS 不能发现入侵行为。

(2) 入侵行为不再是单一的行为，而是表现出相互协作的入侵特点，如分布式拒绝服务攻击(DDoS)。

(3) 入侵检测所依靠的数据来源分散化，收集原始的检测数据变得困难，如交换型网络使得监听网络数据包受到限制。

(4) 网络速度传输加快，网络的流量大，集中处理原始数据的方式往往造成检测瓶颈，从而导致漏检。

基于这样的情况，分布式入侵检测系统就应运而生。

分布式入侵检测系统通常由数据采集构件、通信传输构件、入侵检测分析构件、应急处理构件和管理构件组成。如图 6.3 所示，这些构件可根据不同情形进行组合。

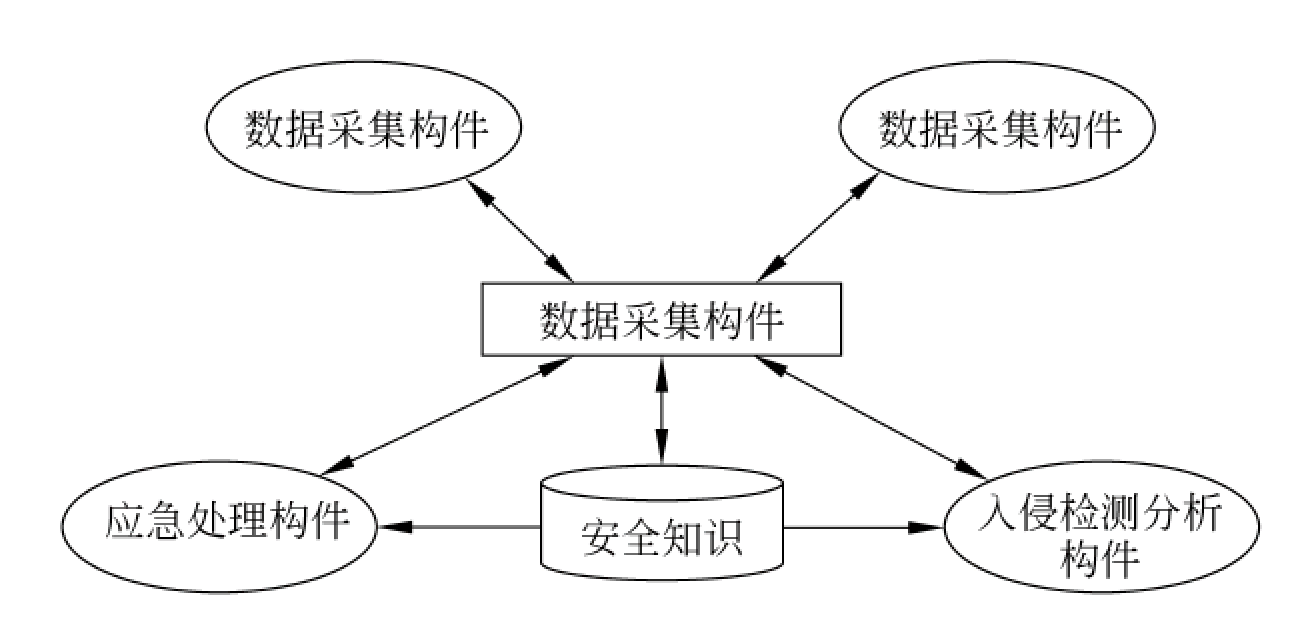


图 6.3 分布式入侵检测系统

3. 混合入侵检测

混合入侵检测系统是基于网络和基于主机的入侵检测系统的结合，这种混合的解决方案为基于主机的入侵检测和基于网络的入侵检测提供了互补，并提供了入侵检测的集中管理。采用这种技术能实现对入侵行为的全方位检测，避免入侵行为被忽略。

4. 网络节点的入侵检测

网络节点入侵检测(network-node intrusion detection，NNID)是为加固传统的网络入侵检测周围环境而开发的，它使用 Sniffer 技术截取从网线上传输给主机的数据包。与网络入侵检测不同的是，网络节点入侵检测是在数据包到达主机后进行截取。网络节点

入侵检测的设想来源于多个基于网络的入侵检测中心理论，即每一个中心主机都必须利用基于主机的技术优势。通常网络节点入侵检测只是简单附在主机入侵检测上的一个模块。

由于嗅探技术的限制，网络节点入侵检测仅仅能分析目的地址是主机地址的包，但是由于网络节点入侵检测的特性，当网络使用的是一个高速通信网络、加密网络或者使用了交换式设备，网络节点入侵检测仍然能对所有的子网进行检测。网络节点入侵检测的优势在于，能有效地抵御针对特定主机的基于包的攻击。

6.3 常用的入侵检测方法

入侵检测系统常用的检测方法有特征检测、统计检测与专家系统。据公安部计算机信息系统安全产品质量监督检验中心的报告，国内送检的入侵检测产品中95%是属于使用入侵模式匹配的特征检测产品，其他5%是采用概率统计的统计检测产品与基于日志的专家知识库型产品。

1. 特征检测

特征检测对已知的攻击或入侵的方式作出确定性的描述，形成相应的事件模式。当被审计的事件与已知的入侵事件模式相匹配时，即报警，原理上与专家系统相仿。其检测方法与计算机病毒的检测方式类似。目前，基于对包特征描述的模式匹配应用较为广泛。该方法预报检测的准确率较高，但对于无经验知识的入侵与攻击行为无能为力。

2. 统计检测

统计模型常用异常检测，在统计模型中常用的测量参数包括审计事件的数量、间隔时间、资源消耗情况等。常用的5种入侵检测统计模型如下。

(1) 操作模型。该模型假设异常，可通过测量结果与一些固定指标相比较得到，固定指标可以根据经验值或一段时间内的统计平均值得到。举例来说，在短时间内多次失败的登录很有可能是口令尝试攻击。

(2) 方差。计算参数的方差，设定其置信区间，当测量值超过置信区间的范围时，表明有可能是异常。

(3) 多元模型。操作模型的扩展，通过同时分析多个参数实现检测。

(4) 马尔柯夫过程模型。将每种类型的事件定义为系统状态，用状态转移矩阵来表示状态的变化，当一个事件发生时，或状态矩阵转移的概率较小则可能是异常事件。

(5) 时间序列分析。将事件计数与资源耗用根据时间排成序列，如果一个新事件在该时间发生的概率较低，则该事件可能是入侵。

统计方法的最大优点是它可以总结用户的使用习惯，从而具有较高检出率与可用性。但是它的总结能力也给入侵者机会，入侵者通过逐步修正使入侵事件符合正常操作的统计规律，从而顺利通过入侵检测系统。

3. 专家系统

用专家系统对入侵进行检测,经常是针对有特征的入侵行为。规则即知识,不同的系统与设置具有不同的规则,且规则之间往往无通用性。专家系统的建立依赖于知识库的完备性,知识库的完备性取决于审计记录的完备性与实时性。入侵的特征抽取与表达,是入侵检测专家系统的关键。在系统实现中,将有关入侵的知识转化为 if-then 结构,条件部分为入侵特征,then 部分是系统防范措施。运用专家系统防范有特征入侵行为的有效性则完全取决于专家系统知识库的完备性。

6.4 常见的入侵检测系统

1. Watcher

Watcher 是一个典型的网络入侵检测工具,它能检测所有通过网络的信息包,并且将其当成恶意的入侵行为记录在 syslog 中,Watcher 能够检测下列的攻击行为。

(1) 所有的 TCP 扫描。

(2) 所有的 UDP 扫描。

(3) Synflood 攻击。

(4) Teardrop 攻击。

(5) Land 攻击。

(6) Smurf 攻击。

(7) Ping of Death 攻击。

所有的参数及配置都是在命令行给出的,可以配置它仅仅监视扫描行为或者仅仅监视 DoS 攻击。它的攻击原理是:如果在短时间内有超过 7 个以上的端口收到信息包,不管类型如何,那么这个事件就被当成端口扫描记录下来。UDP 扫描认定的原理也一样。当 Watcher 所在同一端口收到超过 8 个没有带 ACK 或者 FIN 位的 SYN 包的话,就会被认定是 Synflood 攻击事件。如果 UDP 的碎片包——IP 包的 id 号是 242,它就被认为是 Teardrop 攻击,因为发布的攻击代码使用的是 242 的 id 号。这点存在不足,因为入侵者完全可以自己定义入侵程序的记号。

对同一端口的大量 TCP SYN 包,带源地址及目标地址的,将被认为是 Land 攻击,如果在很短时间内出现不止 5 个 ICMP Echo Replies(时间可以自定义),将记录为 Smurf 攻击。

Watcher 有 3 种监测模式,第一种模式,也是默认的模式,仅仅监测对本台主机的攻击行为;第二种模式可以监测在 C 类子网内的所有主机;第三种模式则可以监测所有能接收到信息包的主机。

当把 Watcher 放在外部主机上时,监测多主机特别有效,当一台主机的 log 文件被破坏时,其他主机上还有记录。由于 Watcher 把所有的信息包都当成“攻击”,然后再进行分析,这种判断是极为粗糙的,可能会误判,所以开发者应在代码中加入一些过滤的技巧。

Watcher 的输出非常简单,每隔 10 秒钟就将可能的攻击行为记录在系统日志中,同时源 IP 及目标 IP 甚至相关的信息(比如端口号、包的数量等)也将被记录下来。但是拒绝服务入侵的包的源地址一般都是伪造的,不过,如果该攻击行为的 IP 地址是假的,那么它会同时记下 MAC 地址。如果攻击来自外部,地址将是本地接收到该包的路由器的地址,如果攻击来自内部的话,就可先抓住攻击者。

Watcher 用于 Linux 系统,一般情况下只需要在命令行后台运行它。

2. Cisco 公司的 NetRanger

NetRanger 产品分为两部分:监测网络包和发布告警的传感器,以及接收并分析告警和启动对策的控制器。NetRanger 以其高性能而闻名,而且它还非常易于裁剪。控制器程序可以综合多站点的信息并监视散布在整个企业网上的入侵。NetRanger 的最大名声在于其是针对企业而设计的。

NetRanger 在全球广域网上运行很成功。它有一个路径备份功能。如果一条路径断掉了,信息可以从备份路径上传过,甚至能做到从一个点上监测全网或把监测权转给第三方。

NetRanger 的另一个强项是当其在检测问题时不仅观察单个包的内部,而且还看上下文,即从多个包中得到线索。这是很重要的一点,因为入侵者可能以字符模式存取一个端口,然后在每个包中只放一个字符。如果一个监测器只观察单个包,它就永远不会发现完整的信息。

NetRanger 是目前市场上基于网络的入侵检测软件中经受实践考验最多的产品之一。但是,对于某些用户来讲,NetRanger 的强项也可能正好是其不足。它被设计为集成在 OpenView 或 NetView 下,在网络运行中心(NOC)使用,配置要求对 UNIX 有详细的了解。NetRanger 相对较昂贵,这对于一般的局域网来说不一定很适合。

3. 入侵检测系统 BlackICE 简介

该软件在 1999 年获得了 PC Magazine 的技术卓越大奖,对于没有防火墙的家庭用户来说,BlackICE 是一道不可缺少的防线;而对于企业网络,它又增加了一层保护措施。它并不是要取代防火墙,而是阻止企图穿过防火墙的入侵者。BlackICE 集成有非常强大的检测和分析引擎,可以识别 200 多种入侵技巧,给用户全面的网络检测及系统防护,它还能即时监测网络端口和协议,拦截所有可疑的网络入侵,无论黑客如何费尽心机也无法危害到系统。而且它还可以将查明那些试图入侵的黑客的 NetBIOS(WINS)名、DNS 名或是他目前所使用的 IP 地址记录下来,以便用户采取进一步行动。该软件的灵敏度和准确率非常高,稳定性也相当出色,系统资源占用率极少,是网络监测的较好的选择。其功能如下。

(1) 增加了应用程序与通信控制的功能。
(2) 可控制应用程序是否在计算机上执行。
(3) 可控制哪些应用程序能与 Internet 通信。
(4) 扫描你的系统,检测所有的系统设置改变。

(5) 可在事件列表中记录新软件与新通信事件的发生情况。



【案例】 BlackICE入侵检测系统的应用

案例分析

BlackICE一款非常强大的入侵检测系统工程,集成有非常强大的检测和分析引擎,能进行全面的网络检测及系统防护,即时监测网络端口和协议,拦截所有可疑的网络入侵,从而提高网络的安全性。

操作环境

(1) 一台连上Internet的计算机。
(2) 入侵检测软件BlackICE。

操作步骤

第1步 BlackICE软件的下载安装。可以在华军软件园等网站下载,本实训以BlackICE PC Protection 3.6为例,下载、解压软件后,运行安装程序即可安装BlackICE。

第2步 熟悉BlackICE软件的界面。

BlackICE软件的界面如图6.4所示。

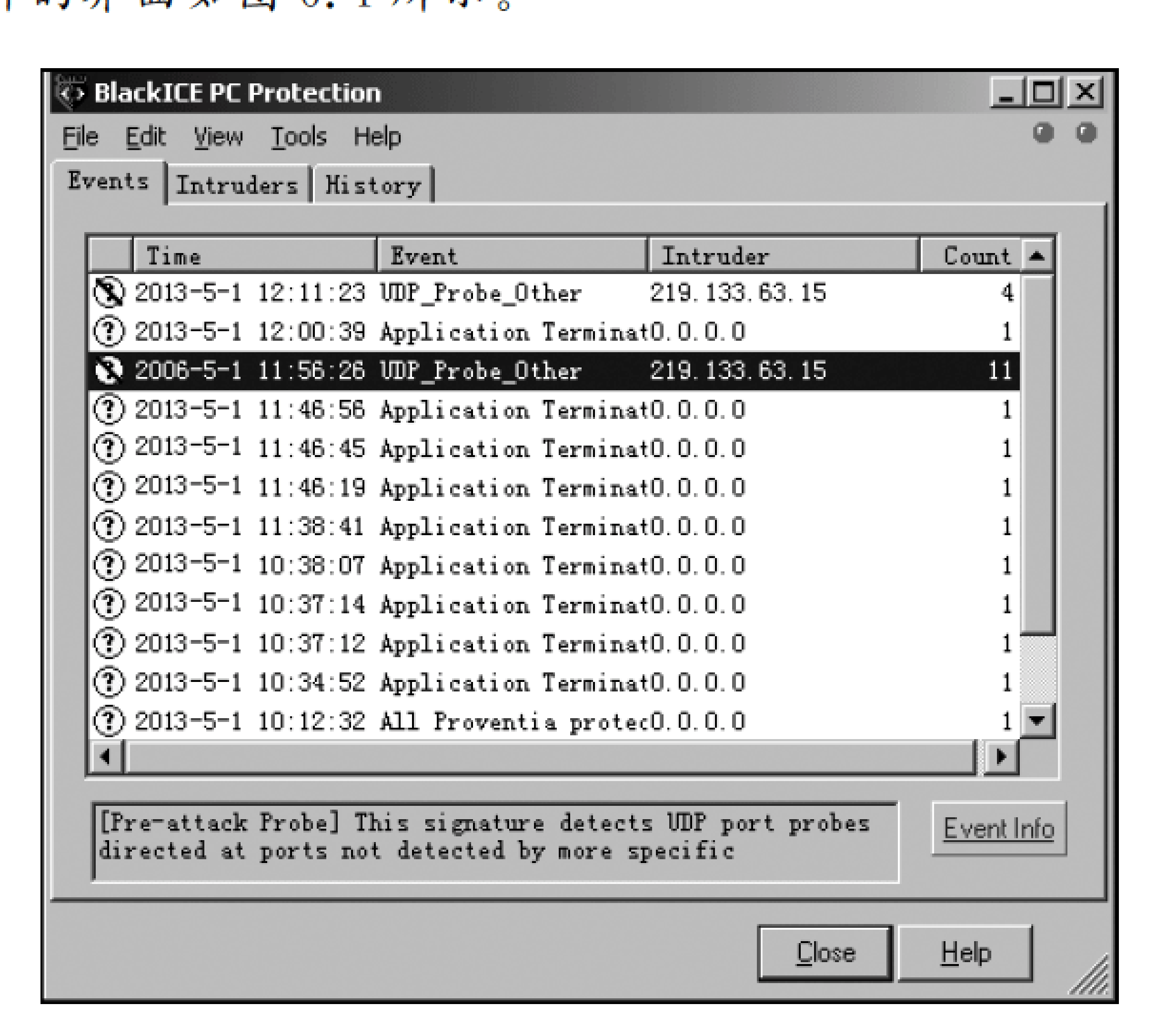


图6.4 BlackICE的界面

(1) 掌握文件栏中菜单的操作内容。
(2) 掌握Events(事件)、Intruders(入侵者)和History(历史)3个书签的信息内容。

第3步 规则设置。

(1) 规则设置与编辑。选择"工具"→"编辑BlackICE设置"命令,出现BlackICE的设置对话框,用户可以根据自己的需要进行配置。

（2）防火墙规则设置。选择"工具"→"高级防火墙设置"命令，出现 Advanced Application Protection Settings 对话框，如图 6.5 所示。根据需要从中可以添加、删除和修改防火墙项目。

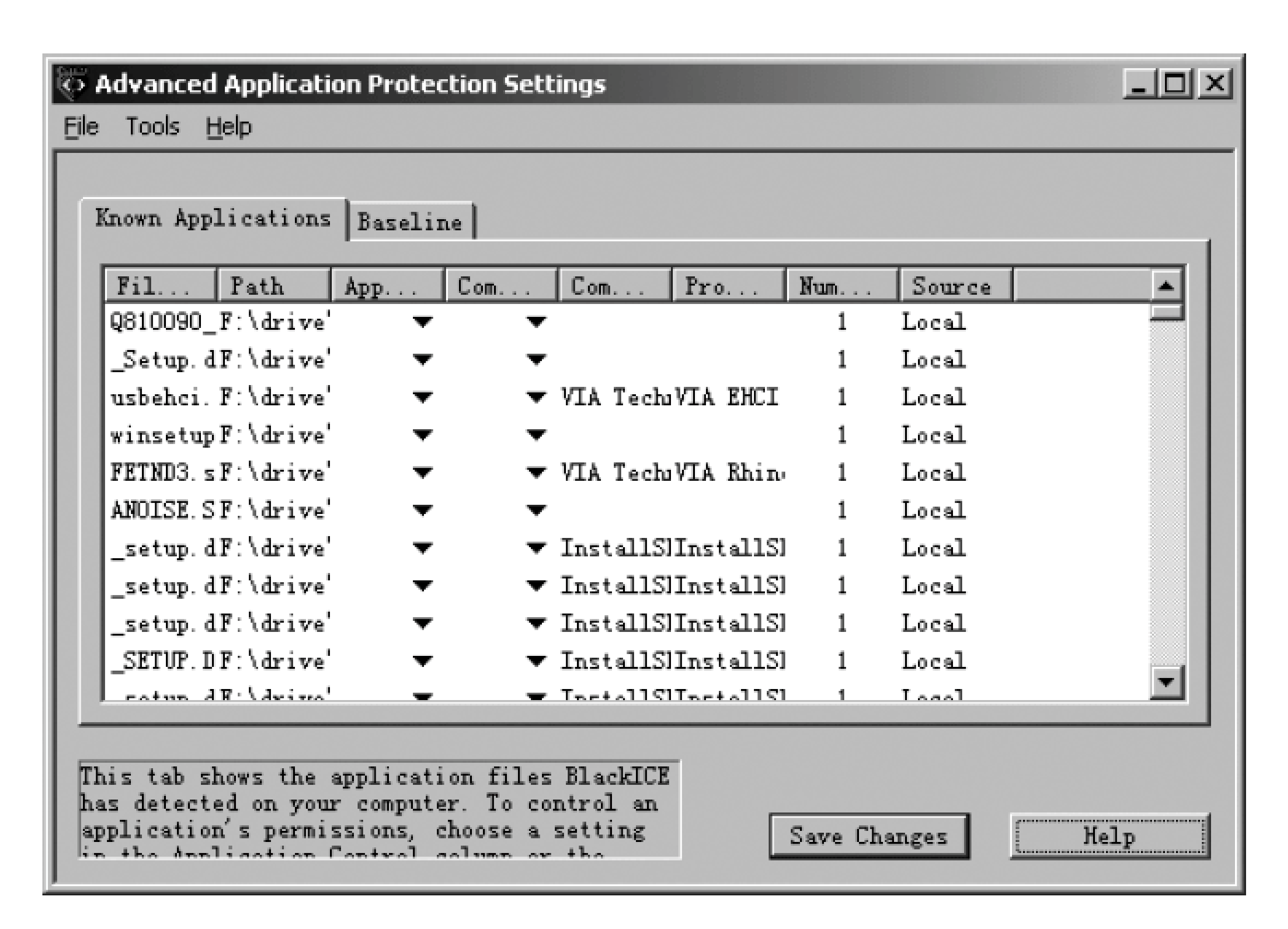


图 6.5　Advanced Application Protection Settings 对话框

（3）查阅"入侵者"信息，如图 6.6 所示。可以直接将入侵者的 IP 地址、计算机名、NetBIOS 名、DNS 名、MAC 地址等显示出来。如果用户确认某个入侵者后，可以在入侵者上右击，拦截选定的入侵者，时间有 4 种选择：1 小时、1 天、1 个月和永久。

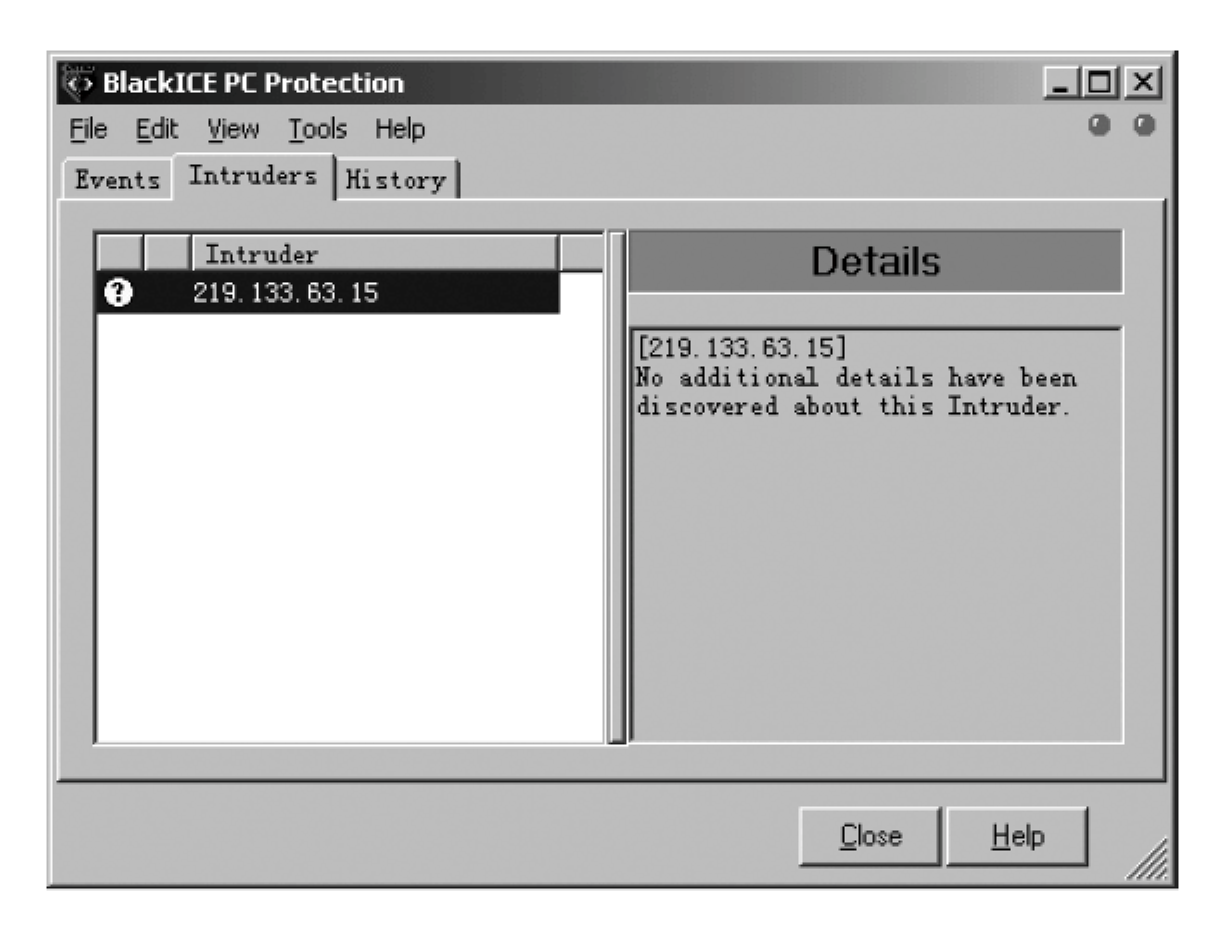


图 6.6　Intruders 选项卡

6.5　入侵检测系统的选购策略

目前基于网络的入侵检测产品有很多，如果不考虑费用问题，可以使用优秀的商业产品，使用这些产品会得到来自开发商的技术支持和产品更新。当然，还有很多非商业化的

产品如Snort这一类的自由软件。选购产品最重要的就是量力而行，而不要因为产品的名气而购买，记住你需要的是适合自己网络使用的入侵检测产品。

当选择入侵检测系统时，要从如下方面考虑。

(1) 系统的价格。价格是必须考虑的要点，不过，性能价格比及要保护系统的价值则是更重要的因素。

(2) 特征库升级与维护的费用。像反病毒软件一样，入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

(3) 对于网络入侵检测系统，最大可处理流量是多少包/秒(p/s)。首先，要分析网络入侵检测系统所安装的网络环境，如果在512KB或24MB专线上安装网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。

(4) 该产品是否容易被躲避。有些常用的躲开入侵检测的方法，如分片、TTL欺骗、异常TCP分段、慢扫描、协同攻击等。

(5) 产品的可伸缩性。系统支持的传感器数目、最大数据库大小、传感器与控制台之间的通信带宽和对审计日志溢出的处理。

(6) 运行与维护系统的开销。产品报表结构、处理误报的方便程度、事件与日志查询的方便程序以及使用该系统所需的技术人员数量。

(7) 产品支持的入侵特征数。不同厂商对检测特征库大小的计算方法都不一样。

(8) 产品有哪些响应方法。要从本地、远程等多个角度考察。自动更改防火墙配置是一个听起来很不错的功能，但是，自动配置防火墙是一个极为危险的举动。

(9) 是否通过了国家权威机构的评测。主要的权威测评机构有中国信息安全测评中心、公安部计算机信息系统安全产品质量监督检验中心。

理想的入侵检测系统方案应该是具有以下特点。

(1) 快速控制台。

(2) 良好的误警报管理。

(3) 显示已经分析过的事件。

(4) 标志已经分析过的事件。

(5) 层层探究的能力。

(6) 关联分析能力。

(7) 报告能力。

从目前情况来看，每天都会有许多新的入侵方式出现，对于入侵事件的检测仅靠入侵检测系统是不现实的，但是也不能完全放弃入侵检测系统。即使是训练有素的专家级分析员也需要通过各种工具才能对这些入侵行为进行分析。一般来说，提供给分析员的信息越多，分析员解决入侵检测问题的机会就越大，但是任何事情都不能走极端，过多的信息也有可能使分析员在大量的信息中迷失，将宝贵的时间和精力浪费在分离大量的无效信息上。因此，合理地选择并部署入侵检测系统才能获得最合理的入侵检测能力。

6.6 入侵检测系统的局限性及发展趋势

1. 入侵检测系统的局限性

入侵检测系统也面临着若干重要的挑战。这些挑战有些来自技术方面，有些则来自非技术方面。

(1) 技术方面

① 网络规模和复杂程序不断增长。在一个大型的异构网络环境中，入侵检测系统所遇到的主要问题有：如何集成并处理来自分布在网络各处实体的具有不同格式的各种相关信息？如何在相互合作但是并不完全相互信任的组织之间来共享敏感的相关入侵行为信息？如何进行管理域间的合作进程及如何保证在局部入侵检测系统失效的情况下仍能维护系统全局的安全等。

② 如何在造成损失前及早发现入侵活动。

③ 网络繁忙情况下的系统性能问题。为了保证发挥效能，网络入侵检测系统必须能够分析所有的内向数据包。如果一个入侵检测系统无法应付网络吞吐量的话，它就可能漏掉不少反映入侵活动的特征数据，从而造成安全漏洞。

④ 入侵模式特征的准确性。用来描述异常入侵行为的模式特征是滥用检测系统最重要的基石。如何保证所采用的特征集能够准确而又足以描述已知的各种攻击模式(包括复杂的分阶段攻击行为)及其变种，是一个重要而敏感的问题。

⑤ 入侵检测系统的评估。对入侵检测系统评估测试是一项复杂的工作，因为 IDS 不能在独立环境中检测，首先必须建立一个实际网络平台环境。同时，还需要大量的包含各种测试入侵的复杂数据，这些数据还要根据不同的操作系统平台和版本加以调整。时至今日，在这方面所做的工作非常少。

(2) 非技术方面

① 攻击者不断研究新的攻击模式，同时，随着安全技术的普及，越来越多的人进行了越来越多的入侵攻击尝试。自动攻击的软件工具不断得到改进，使普通用户也能够利用它来进行网络攻击。各种机构(包括政府、公司等)对包括 IDS 在内的安全技术的认识不足或者缺乏足够熟练的安全管理员。

② 我国计算机系统及网络产品以国外的为主，软/硬件系统中难免存在各种潜在威胁和安全“陷阱”(诸如操作系统后门、路由器漏洞等)，因此，利用这些设备建立的网络系统，在其安全性方面得不到根本性的保障。

2. 入侵检测的发展趋势

入侵检测系统与其他的网络产品一样，在过去几年获得了非常大的发展，入侵检测系统已经成为维护网络安全的重要产品，就如同防火墙一样。不过，未来是很难预料的，网络的情况会改变，入侵者也在不断地学习。入侵检测系统必须要面对这些问题，并不断地演化以适应环境的变化。无论如何，管理员都必须确信入侵检测系统是帮助他们维护网

络安全最有力的武器之一。下面几点是未来对入侵检测发展可能带来影响的因素。

(1) 安全事件逐年上升

对管理员而言,将网络接入 Internet,就意味着将网络暴露在全球的入侵者面前,大量的攻击行为将使入侵检测系统面临更大的压力。

(2) 安全问题日渐增多

Internet 的不断发展使网络日趋复杂,软件的功能不断增加,然而安全漏洞被发现的数量也不断扩大。除了操作系统外,各种服务软件的漏洞都有可能给系统带来安全方面的威胁。入侵检测系统必须具备足够的能力跟踪最新的漏洞出现。

(3) 良好的适应性

网络入侵检测系统通过匹配网络数据包发现攻击行为,入侵检测系统往往假设攻击信息是通过明文传输的,因此,对信息稍加改变便可能骗过入侵检测系统的检测。一些攻击者已经开始利用这一点通过加密的方法传输控制信息。还有许多系统通过 VPN(虚拟专用网)进行网络之间的互联,如果入侵检测系统不了解其所用的隧道机制,就会无法发现可能存在的入侵行为。

(4) 必须协调、适应多样性的环境中的不同的安全策略

网络及其中的设备越来越多样化,既存在关键资源,如邮件服务器、企业数据库,也存在很多相对不是很重要的个人计算机;不同企业之间的这种情况也不尽相同。所以入侵检测系统要能适应多样的环境要求。

本 章 小 结

入侵检测系统是网络安全保障体系结构中的重要环节,它为实时安全事件审计、发现攻击入侵行为、采取及时的响应措施、避免系统受到进一步的危害提供了技术保障。

从功能上讲,入侵检测系统由探测器、分析器和用户接口组成。

入侵检测系统的数据来源可以来自多方面,针对这些安全审计数据源,入侵检测系统可以采取模式匹配、统计分析等误用检测或异常检测技术,对入侵行为做出及时判断,帮助系统管理员更好地维护系统安全。

本 章 练 习

一、填空题

1. 入侵检测系统是________的系统。
2. 入侵检测系统的需求特性有________性、________性、________性、________性和________性。
3. 从功能上讲,入侵检测系统由________、________和________三部分组成。
4. 网络入侵检测是通过分析________来工作的。
5. 混合入侵检测系统是________和________入侵检测系统的结合。

二、选择题

1. 入侵检测利用的信息分析包括________。
   A. 系统和网络日志文件
   B. 目录和文件中的不期望的改变和程序执行中的不期望的行为
   C. 物理形式的入侵信息
   D. 以上所有信息
2. 用于事后分析的入侵检测方法是________。
   A. 模式匹配　　B. 统计分析　　C. 完整性分析　　D. 可靠性分析
3. 一个基于网络的入侵检测程序用________去检测攻击。
   A. 一次攻击的分析　　B. DNS 的配置
   C. 特征数据库　　D. 包探测器
4. 一个基于网络的入侵检测程序最适合检测________。
   A. 直接攻击和木马攻击　　B. 直接攻击和拒绝服务攻击
   C. 端口扫描和拒绝服务攻击　　D. 拒绝服务攻击和木马攻击
5. 一个基于网络的入侵检测程序探测离开网络的数据包,系统的________最重要。
   A. 网卡的质量　　B. 系统的制造商
   C. 系统的显示器　　D. 内存的质量

三、简答题

1. 入侵检测系统的作用有哪些?
2. 入侵检测系统由哪些部分组成?
3. 简述入侵检测系统发展的动态和趋势。
4. 如何选购入侵检测系统?

实训　Snort 入侵检测工具的应用

实训目的

了解入侵检测的基本概念,掌握 Snort 入侵检测工具的使用。

实训环境

(1) Snort 入侵检测系统、SQL 数据库系统。
(2) Windows Server 2003 系统。

实训步骤

第 1 步　安装 Apache。
选择定制安装,安装路径修改为 C:\apache,这样与后面的参数设置保持一致。

在命令行窗口输入下面的命令，启动 Apache 服务。

```
Net shart apache2
```

第 2 步 安装 PHP。

(1) 解压缩 php-4.3.2-Win32.zip 至 C:\php。

(2) 复制 php4ts.dll 至 C:\WINDOWS\system32。

(3) 复制 php.ini-dist 至 C:\WINDOWS\php.ini。

(4) 修改 php.ini。

```
extension=php_gd2.dll
```

(5) 复制 C:\php\extension\php_gd2.dll C:\WINDOWS\(注：以上添加 gd 图形库支持)。

(6) 在 httpd.conf 中添加：

```
LoadModule php4_module"c:/php/sapi/php4apache2.dll"
AddType application/x-httpd-phd.phd
```

(7) 在 C:\apache2\htdocs 目录下新建 test.php 文件，test.php 文件的内容为 <? phpinfo()? >。

(8) 打开浏览器，输入 http://127.0.0.1/test.php，测试 PHP 是否安装成功，安装成功后的页面如图 6.7 所示。

PHP Version 4.3.9	
System	Windows NT ZUGA 5.0 build 2195
Build Date	Sep 21 2004 14:03:10
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINNT\php.ini
PHP API	20020918
PHP Extension	20020429
Zend Extension	20021010
Debug Build	no
Thread Safety	enabled
Registered PHP Streams	php, http, ftp, compress.zlib

图 6.7 PHP 安装成功的界面

第 3 步 安装配置 MySQL 数据库。

默认安装到 C:\mysql，新建 my.ini 并复制到 C:\WINDOWS\下，其中 my.ini 的内容如下。

```
[mysqld]
basedir=c:\mysql
bind-address=127.0.0.1
datadir=c:\mysql\data
```

启动 MySQL 服务，在命令行窗口执行如下命令：

```
mysql-install
net start mysql
```

配置 root 口令：

```
c:\>cd mysql\bin
c:\mysql\bin>mysql
mysql>set password for"root"@ "localhost"=password('newPWD');
```

注意：这里 newPWD 为此处用户自己设置的密码。

以 root 身份登录：

```
Mysql -u root -p
```

第 4 步 安装 Snort。

默认安装到 C：\snort 下，然后在命令行窗口下输入下面的命令，建立 Snort 运行必需的 snort 库和 snort_archive 库。

```
mysql>create database snort;
mysql>create database snort_archive;
```

在命令行使用 C：\snort\contrib 目录下的 create_mysql 脚本建立 Snort 运行必需的数据表。

```
c:\mysql\bin\mysql-D snort-u root-p<c:\snort\contrib\ create_mysql;
c:\ mysql\bin\mysql-D snort_archive - u root - p<c:\snort\contrib\create_mysql;
```

在命令窗口建立 acid 和 snort 用户，或者以 phpmyadmin 用户进行操作。

```
mysql>grant usage on*.* to"acid"@"localhost"identified by "acidpassword";
mysql>grant usage on*.* to"snort"@ localhost" identifies by "snortpsaaword";
```

然后为 acid 用户和 snort 用户分配相关的权限。

```
mysql>grant select,insert,update,delete,create,alter on snort . * to"acid"@"localhost";
mysql>grant select,insert on snort .* to"snort"@"localhost";
mysql>grantselect,insert,update,delete,create,alter on snort_archive .* to "acid" @"localhost";
```

这一步也可以以 phpmyadmin 用户进行操作。

第 5 步 安装配置 adodb、acid。

解压缩 adodb360. zip 至 C：\php\adodb 目录下，解压缩 acid-0. 9. 6b23. tar. gz 至 C：\apache2\htdocs\acid 目录下。

修改 acid_conf. php 文件：

```
$DBlib_path="c:\php\adodb";
$alert_dbname="snort";
$alert_host="localhost";
$alert_port=" ";
$alert_user="acid";
$alert_password="acidpassword";
/* Archive DB connection parameters */
$archive_dbname="snort_archive";
$archive_host="localhost";
$archive_port=" ";
$archive_user="acid";
$archive_password="acidpassword";
$ChartLib_path="c:\php\jpgraph\src";
```

打开浏览器，输入 http：//127. 0. 0. 1/acid/acid_db_setup. php，按照系统提示建立 acid 运行必需的数据库。

第 6 步 安装 jpgrapg 库。

解压缩 jpgraph-1.12.2.tar.gz 至 C：\php\jpgraph。

修改 jpgraph.php：

```
DEFINE("CACHE_DIR","/tmp/jpgraph_cache/")(取消原来的注释)
```

第 7 步 安装 WinPcap。

第 8 步 配置 Snort。

编辑 C：\snort\etc\snort.conf，需要将修改。

```
include classification.config
include reference.config
```

修改为绝对路径：

```
include c:\snort\etc\classification.config
include c:\snort\etc\reference.config
```

设置 snort 输出 alert 到 MySQL Server。

```
output database: alert, mysql, host=localhost user=snort password=snort dbname=snort
```

第 9 步 测试 Snort。

输入命令，运行 Snort。

```
c:\snort\bin>snort - c "c:\snort\etc\snort.conf"-l"c:\snort\log" - vdeX
```

其中：

-X 参数用于在数据链接层记录 raw packet 数据。

-d 参数记录应用层的数据。

-e 参数显示/记录第二层报文头数据。

-c 参数用以指定 Snort 的配置文件和路径。

-v 参数用于在屏幕上显示被抓到的包。

启动 Apache 和 MySQL 服务。

```
net start apache2
mysqld-install
net start mysql
```

运行 acid：打开浏览器，地址为 http：//127.0.0.1/acid。若如图 6.8 所示，则表示 acid 安装成功。

在命令行运行 Snort，在运行中输入命令：

```
c:\snort\bin\snort-c "c:\snort\etc\snort.conf"-l"c:\snort\log" -de
```

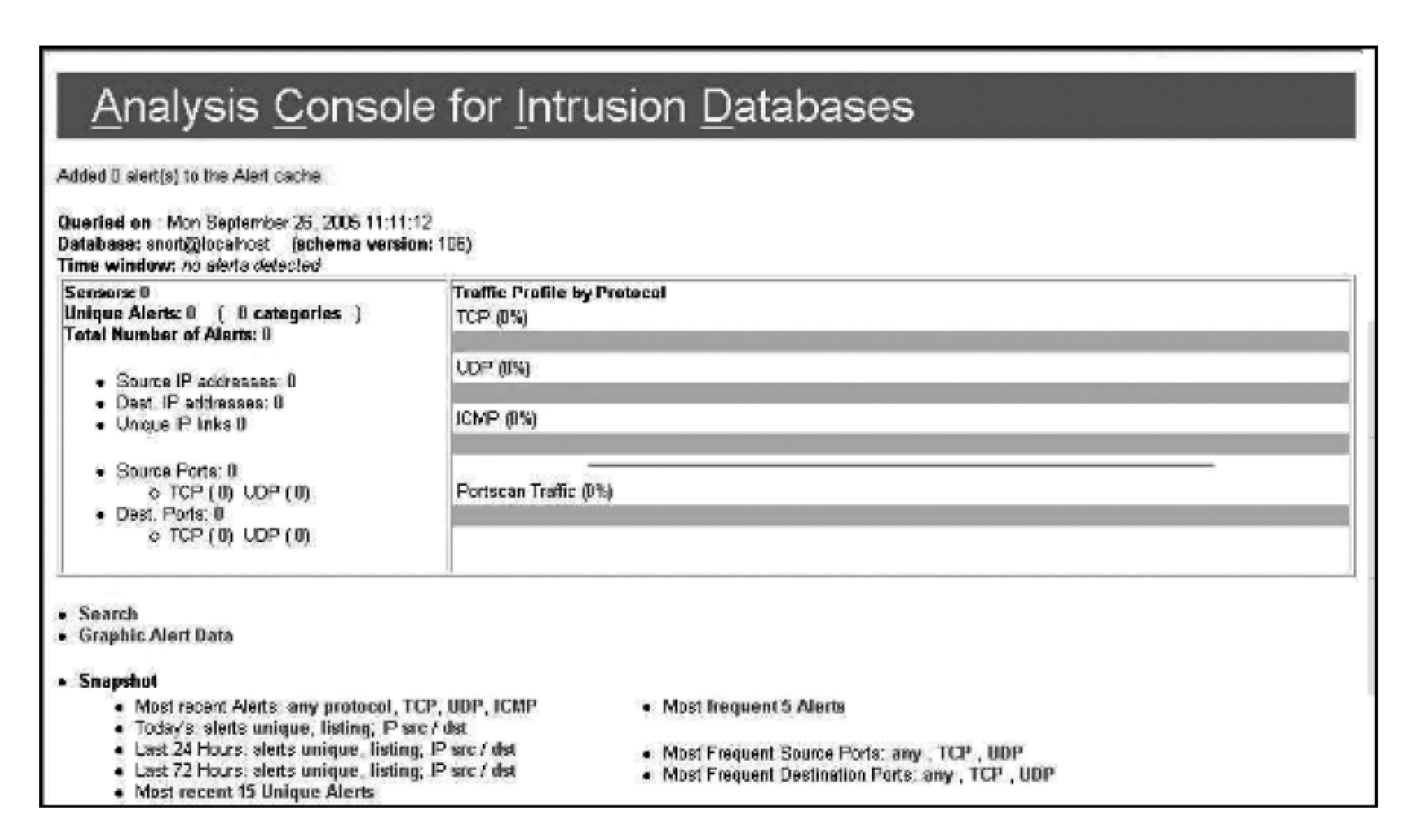


图 6.8　acid 安装成功

如果 Snort 正常运行，则如图 6.9 所示。

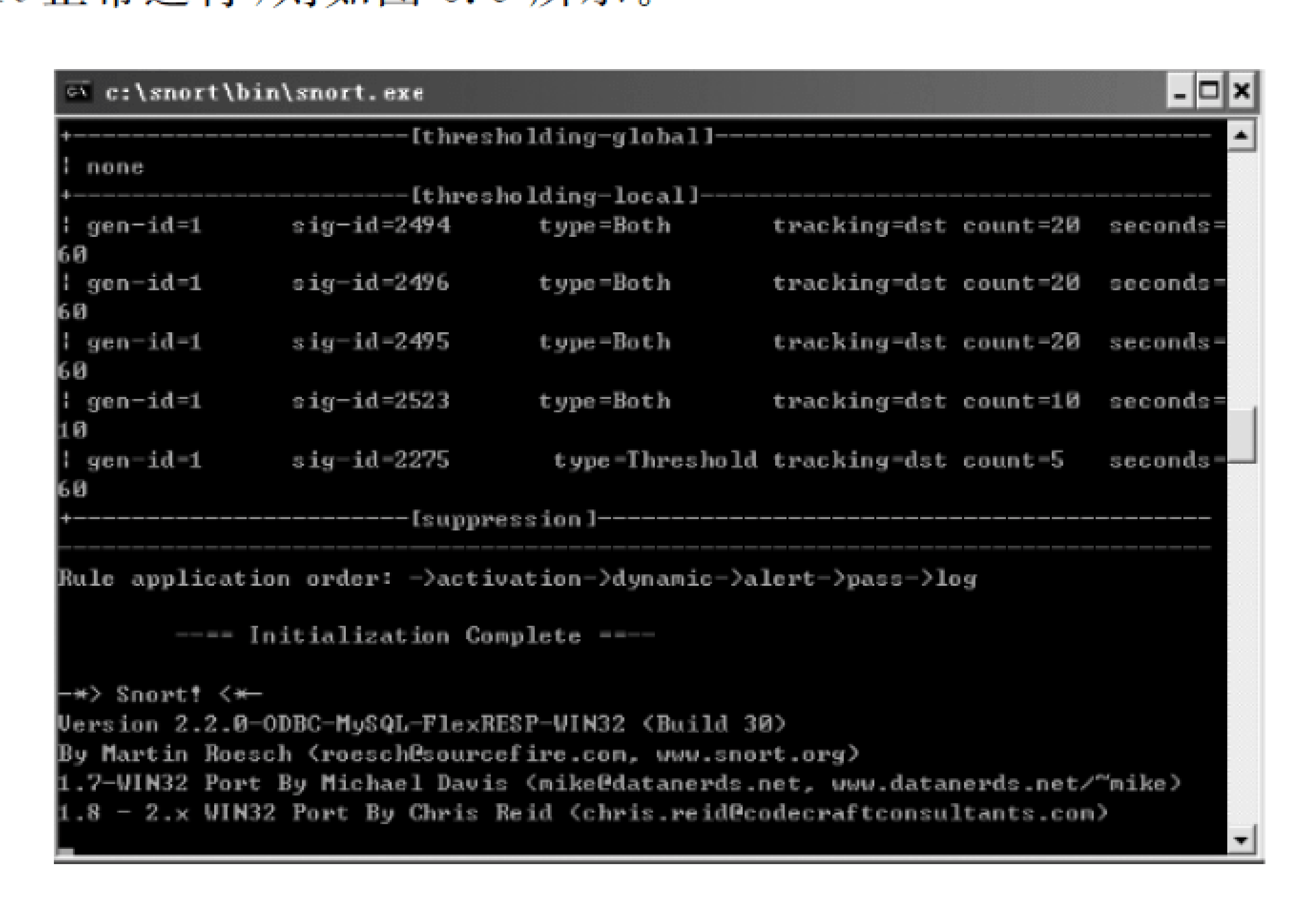


图 6.9　Snort 正常运行界面

第 10 步　开始检测。

首先配置 snort.conf 文件，将 var HOME_NET any 语句中的 any 改为自己所在的子网地址，即将 snort 监测的内网设置为本机所在局域网。接下来，设置 snort.conf 文件中的 rule 规则，将#include 前的#去掉，表示启用此条规则。

参照第 9 步，启动 Snort 并用浏览器打开 acid 控制台，单击 TCP 后的数字，将显示所有检测到的 TCP 协议和数据包的详细情况，如图 6.10 所示。

不要关闭 Snort，打开 superscan 对检测网段进行扫描，再打开 acid 查看检测结果。

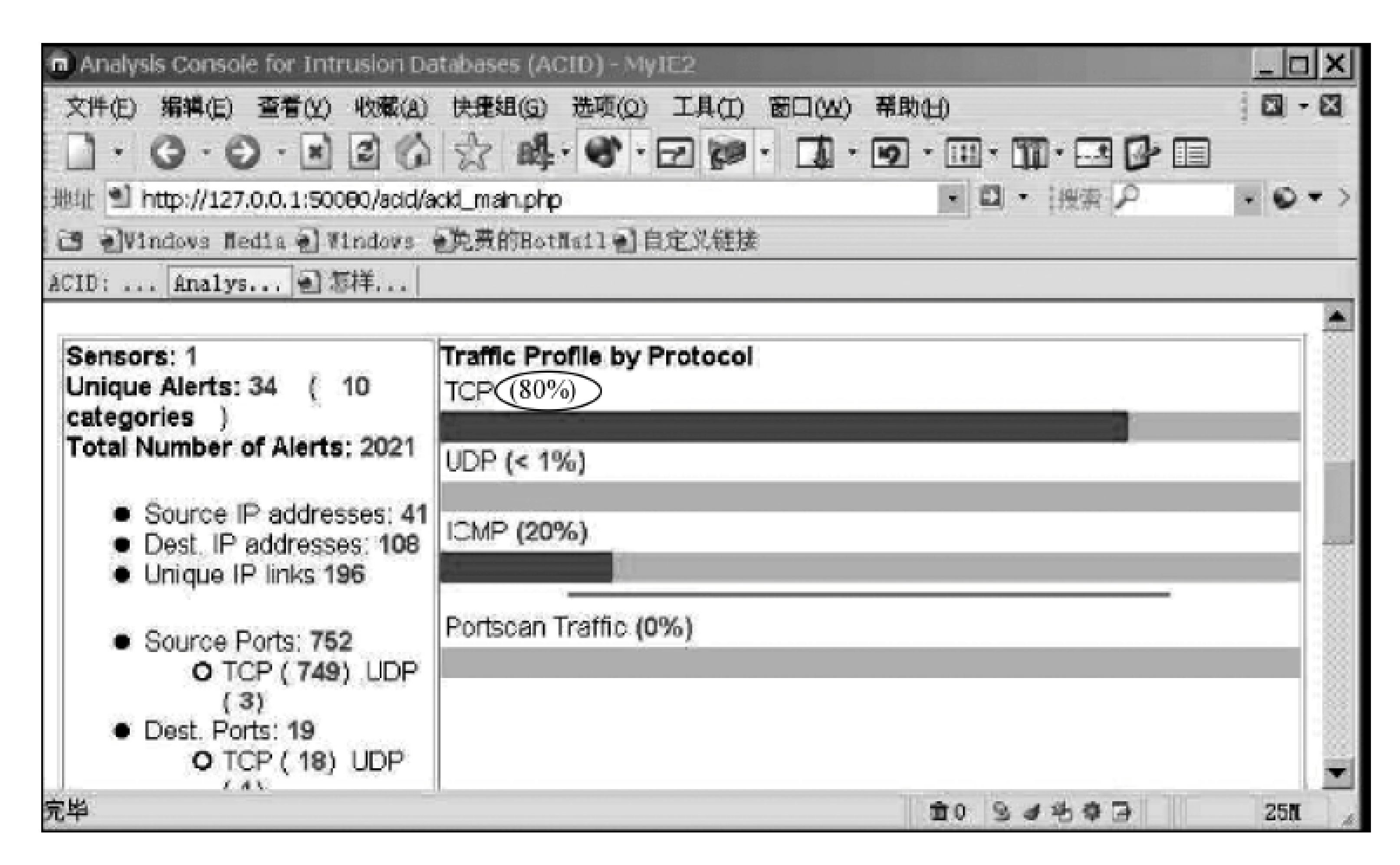

Analysis Console for Intrusion Databases (ACID) - MyIE2
http://127.0.0.1:50080/acid/acid_main.php
Sensors: 1
Unique Alerts: 34 (10 categories)
Total Number of Alerts: 2021
Source IP addresses: 41
Dest. IP addresses: 108
Unique IP links 196
Source Ports: 752
TCP (749) UDP (3)
Dest. Ports: 19
TCP (18) UDP
Traffic Profile by Protocol
TCP (80%)
UDP (< 1%)
ICMP (20%)
Portscan Traffic (0%)
完毕

图 6.10　显示信息

第 7 章

网络病毒的防范与清除

Chapter 7

知识目标

- 掌握计算机病毒的定义、分类、特点及防治。
- 掌握常用杀毒软件的使用。
- 了解典型网络病毒的特点。

技能目标

- 能够使用常用杀毒软件防范与清除病毒。
- 能够清除与防范典型网络病毒。

计算机的普及和网络的发展，使得计算机病毒的防治更加重要。早期病毒的传播媒介主要是软盘，进入 Internet 时代后，网络又成为计算机病毒最好的传播途径。病毒扩散速度之快也是前所未有的，它严重威胁着网络的安全。

7.1 计算机病毒的基础知识

7.1.1 计算机病毒的定义

早在 1949 年，计算机先驱者冯・诺伊曼就在他的论文《复杂计算机组织论》中，提出了计算机程序能够在内存中自我复制，勾勒出了病毒程序的蓝图。

1983 年 11 月 3 日，弗雷德・科恩博士研制出了一种在运行过程中可以自我复制的破坏性程序，伦・艾德勒曼将它命名为计算机病毒，并在每周一次的安全讨论会上正式提出，会议结束 8 小时后专家们在 VAX11/750 计算机系统上运行，第一个病毒实验成功，一周后获准推出 5 个实验的演示，从而在实验上验证了计算机病毒的存在。

1985 年年初，在巴基斯坦的拉合尔，巴西特和阿姆杰得两兄弟为了防盗版，编写了“巴基斯坦智囊”病毒，该病毒传染软盘引导，一年后病毒以强劲势头流传到了全世界。这是最早在世界上流行的一个真正的病毒。几乎同时，世界各地的计算机用户也发现了形形色色的计算机病毒，如黑色星期五、大麻等。

“计算机病毒”的概念是由美国计算机研究专家 F. Cohen 最早提出来的，像生物病毒一样，计算机病毒具有独特的复制能力。它们能把自身附在各种类型的文件上，当文件被

复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。除复制能力之外，某些计算机病毒还有其他一些共同特性：一个被感染的程序能够传送病毒载体。当你看到病毒载体似乎仅仅表现在文字和图像上时，它们可能已经毁坏了文件、格式化了硬盘或引发了其他类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存储空间给我们带来麻烦，并降低计算机的性能。

出现在计算机领域中的计算机病毒是一组程序，一段可执行码，是一种隐藏在计算机系统的可存取信息资源中，利用系统信息资源进行繁殖并且执行的编码集合。计算机病毒在《中华人民共和国计算机信息系统安全保护条例》中明确定义为："指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据、影响计算机使用，并能够自我复制的一组计算机指令或者程序代码。"此定义具有法律性、权威性。

【资料链接】 计算机病毒的命名

反病毒公司为了方便管理，用了一个大致统一的命名方法按照病毒的特性对病毒进行分类命名。了解病毒命名规则，对我们了解、防范、清除病毒很有利。

一般格式为：＜病毒前缀＞.＜病毒名＞.＜病毒后缀＞。

病毒前缀是指一个病毒的种类，是用来区别病毒的种族分类的。不同的种类的病毒，其前缀也是不同的，如常见的木马病毒的前缀是 Trojan ，蠕虫病毒的前缀是 Worm 等。

病毒名是指一个病毒的家族特征，是用来区别和标识病毒家族的，如振荡波蠕虫病毒的家族名是 Sasser。

病毒后缀是指一个病毒的变种特征，用来区别具体某个家族病毒的某个变种。一般都采用英文中的 26 个字母来表示，如 Worm. Sasser. b 就是指振荡波蠕虫病毒的变种 B，因此一般称为"振荡波 B 变种"或者"振荡波变种 B"。如果该病毒变种非常多，可以采用数字与字母混合表示变种标识。

1. 系统病毒

系统病毒的公有的特性一般是可以感染 Windows 操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播，如 CIH 病毒。

2. 蠕虫病毒

蠕虫病毒的前缀是 Worm。这种病毒的公有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性，如冲击波(阻塞网络)、小邮差(发带毒邮件)等。

3. 木马病毒、黑客病毒

木马病毒的前缀是 Trojan，黑客病毒的前缀一般为 Hack。木马病毒的公有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的计算机进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的计算机，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型都越来越趋向于整合了。一般的木马如 QQ 消息尾巴木马 Trojan. QQ3344 ，针对网络游戏的木马病毒如 Trojan. LMir. PSW. 60。这里补充一点，病毒名中有 PSW 或者什么 PWD 之类的一般都表示这个病毒有盗取密码的功能(这些字母一般都

为"密码"英文"password"的缩写),而黑客程序则有网络枭雄(Hack. Nether. Client)等。

4. 脚本病毒

脚本病毒的前缀是Script。脚本病毒的公有特性是使用脚本语言编写,通过网页进行的传播的病毒,如红色代码(Script. Redlof)。脚本病毒还会有VBS、JS(表明是何种脚本编写的)等前缀,如欢乐时光(VBS. Happytime)、十四日(Js. Fortnight. c. s)等。

5. 宏病毒

其实宏病毒也是脚本病毒的一种,由于它的特殊性,因此在这里单独算成一类。宏病毒的前缀是Macro,第二前缀是Word、Word 97、Excel、Excel 97其中之一。凡是只感染Word 97及以前版本Word文档的病毒采用Word 97作为第二前缀,格式是Macro. Word 97;凡是只感染Word 97以后版本Word文档的病毒采用Word作为第二前缀,格式是Macro. Word;凡是只感染Excel 97及以前版本Excel文档的病毒采用Excel 97作为第二前缀,格式是Macro. Excel 97;凡是只感染Excel 97以后版本Excel文档的病毒采用Excel作为第二前缀,格式是Macro. Excel,以此类推。该类病毒的公有特性是能感染Office系列文档,然后通过Office通用模板进行传播,如著名的美丽莎(Macro. Melissa)。

6. 后门病毒

后门病毒的前缀是Backdoor。该类病毒的公有特性是通过网络传播,给系统开后门,给用户计算机带来安全隐患,如IRC后门Backdoor. IRCBot。

7. 病毒种植程序病毒

这类病毒的公有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下,由释放出来的新病毒产生破坏,如冰河播种者(Dropper. BingHe2. 2C)、MSN射手(Dropper. Worm. Smibag)等。

8. 破坏性程序病毒

破坏性程序病毒的前缀是Harm。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击,当用户点击这类病毒时,病毒便会直接对用户计算机造成破坏,如格式化C盘(Harm. formatC. f)、杀手命令(Harm. Command. Killer)等。

9. 玩笑病毒

玩笑病毒的前缀是Joke,也称恶作剧病毒。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击,当用户点击这类病毒时,病毒会做出各种破坏操作来吓唬用户,其实病毒并没有对用户计算机进行任何破坏,如女鬼(Joke. Girlghost)病毒。

10. 捆绑机病毒

捆绑机病毒的前缀是Binder。这类病毒的公有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如QQ、IE捆绑起来,当用户运行这些捆绑病毒时,表面上看是运行这些应用程序,实际是运行捆绑在一起的隐藏的病毒,从而给用户造成危害,如捆绑QQ (Binder. QQPass. QQBin)、系统杀手(Binder. killsys)等。

11. 其他少见的病毒前缀

有时候还会看到一些其他的病毒前缀,具体如下。

DoS:会针对某台主机或者服务器进行DoS攻击。

Exploit:会自动通过溢出对方或者自己的系统漏洞来传播自身,或者他本身就是一

个用于Hacking的溢出工具。

HackTool:黑客工具,本身并不破坏计算机系统,但是会被别人加以利用来用你做替身去破坏别人。

7.1.2 计算机病毒的特性

在计算机病毒所具有的特征中,传染性、潜伏性、触发性和破坏性是它的基本特征。它还有隐蔽性、针对性、衍生性和不可预见性等特征。

1. 传染性

病毒的传染性也称为自我复制和可传播性,这是计算机病毒的本质特征。在一定条件下,病毒通过某种渠道从一个文件或一台计算机传染到另外没有被感染的文件或计算机,轻则造成被感染的计算机数据或工作失常;重则使计算机瘫痪。病毒代码就是靠这种机制大量传播和扩散的。携带病毒代码的文件称为计算机病毒载体或带毒程序。每一台被感染了病毒的计算机,本身是一个受害者,又是计算机病毒的传播者,通过各种可能的渠道,如光盘、活动硬盘、网络去传染其他的计算机。在染毒的计算机上曾经使用过的U盘,很有可能已被计算机病毒感染,如果拿到其他机器上使用,病毒就会通过带毒软盘传染这些机器。如果计算机已经联网,通过数据或程序共享,病毒就可以迅速传染与之相连的计算机,若不加以控制,就会在很短的时间内传遍整个世界。

2. 潜伏性

病毒的潜伏性是指具有依附于其他媒体寄生的能力。一个编制巧妙的病毒程序,可以在几周或几个月内进行传播和再生而不被发觉。在此期间,系统的备份设备复制病毒程序,生成程序或数据的副本并送到其他的部位使之传染。大部分的病毒在感染系统之后一般不会马上发作,它可长期隐藏在系统中,只有在满足其特定条件时才启动其表现(破坏)模块。只有这样,它才能进行广泛的传播。如著名的"黑色星期五"病毒在每逢13号的星期五发作。国内的"上海一号"病毒会在每年3、6、9月的13号发作。这些病毒在平时会隐藏得很好,只有在发作日才会露出本来面目。

3. 触发性

触发性是指计算机病毒的发作一般都有一个激发条件,即一个条件控制。这个条件根据病毒编制者的要求可以是日期、时间、特定程序的运行或程序的运行次数等。

4. 破坏性

任何病毒只要侵入系统,都会对系统及应用程序产生程度不同的影响。轻者会降低计算机工作效率,占用系统资源,重者可致系统崩溃。由此特性可将病毒分为良性病毒与恶性病毒。良性病毒可能只显示些画面或播出点音乐、无聊的语句,或者根本没有任何破坏动作,但会占用系统资源。这类病毒较多,如GENP、小球、W-BOOT等病毒。恶性病毒则有明确的目的,或破坏数据、删除文件或加密磁盘、格式化磁盘,有的对数据造成不可挽回的破坏。

5. 隐蔽性

病毒一般是指编写巧妙、短小精悍的程序。通常附在正常程序中或磁盘较隐蔽的地方,也有个别的以隐含文件形式出现,目的是不让用户发现它的存在。系统被感染病毒后,一般情况下用户是感觉不到它的存在的,只有其发作,出现不正常反应时用户才知道。

6. 针对性

计算机病毒是针对特定的计算机和特定的操作系统的。例如,有针对 IBM/PC 及其兼容机的,有针对 Apple 公司的 Macintosh 的,还有针对 UNIX 操作系统的。如小球病毒是针对 IBM PC 及其兼容机上的 DOS 操作系统的。

7. 衍生性

这种特性为病毒制造者提供了一种创造新病毒的捷径。分析计算机病毒的结构可知,传染的破坏部分反映了设计者的设计思想和设计目的,但是,这可以被其他掌握原理的人以其个人的企图进行任意改动,从而衍生出一种不同于原版本的新的计算机病毒(又称为变种),这就是它的衍生性。这种变种病毒造成的危害可能比原版病毒严重得多。

8. 不可预见性

不同种类病毒的代码千差万别,病毒的制作技术也在不断地提高,病毒相比反病毒软件永远是超前的。新的操作系统和应用系统的出现,软件技术的不断发展,也为计算机病毒提供了新的发展空间,对未来病毒的预测更加困难,这就要求人们不断提高对病毒的认识,增强防范意识。

7.1.3 计算机病毒的种类

从第一个病毒出世以来,病毒的数量在不断增加。据国外统计,计算机病毒以每周 10 种的速度递增。按照基本类型划分,可归纳为 6 种类型,即引导型病毒、可执行文件病毒、宏病毒、混合型病毒、特洛伊木马病毒和网页病毒。

1. 引导型病毒

引导型病毒主要感染软盘、硬盘的引导扇区或主引导扇区,在用户对磁盘进行读写操作时进行感染活动。我国流行的引导型病毒有 Anti-CMOS、GENP/GENB、Stone、Torch、Monkey 等。

2. 可执行文件病毒

可执行文件病毒主要感染可执行文件(对于 DOS 或 Windows 来说是感染.COM 和.EXE 等可执行文件)。被感染的可执行文件在执行的同时,病毒被加载并向其他正常的可执行文件传染。像我国流行的 Die_Hard、DIR Ⅱ 等病毒都属此列。

3. 宏病毒

宏病毒是利用高级语言——宏语言编制的病毒。宏病毒仅向 Word、Excel、Access、PowerPoint 和 Project 等办公自动化程序编制的文档进行传染，而不会传染给可执行文件。由于这些办公处理程序在全球存在着广泛的用户，大家频繁使用这些程序编制文档、电子表格和数据库，并通过磁盘、Internet 进行交换，所以，宏病毒的传播十分迅速并非常广泛。国内流行的宏病毒有 TaiWan1、Concept、Simple2、ethan、7 月杀手等。我们所说的蠕虫病毒也属于宏病毒范围。

4. 混合型病毒

顾名思义，混合型病毒是以上几种病毒的混合。混合型病毒的目的是为了综合利用以上 3 种病毒的传染渠道进行破坏。国内流行的混合型病毒有 One_half、Casper、Natas、Flip 等。

5. 特洛伊木马病毒

特洛伊木马病毒也叫黑客程序或后门病毒。一般这种病毒分成服务器端和客户端两部分，如计算机网络中服务器端被此程序感染，别人可通过网络中其他计算机任意控制此计算机，并获得重要文件。国内流行的此类病毒有 BO、NETSPY 等。

6. 网页病毒

随着 Internet 的发展，网络技术逐渐被广泛应用，某些病毒虽然从现在的发展情况来看并不能破坏硬盘上的资料，但是，如果用户使用浏览器来浏览含有这些病毒的网页，浏览器就会把这些程序抓下来，然后用用户系统里的资源去执行，在神不知鬼不觉的状态下，病毒进入用户的计算机进行复制并通过网络窃取宝贵的个人信息，或使计算机系统资源利用率下降，造成死机现象。并且该病毒会在一台一台的终端上不断传播。

7.1.4 计算机病毒的工作原理

认清计算机病毒的结构和主要特征，了解计算机病毒的工作的一般过程及原理，可以为我们检测和清除病毒提供充实、可靠的依据，针对每个环节做出相应的防范措施。

1. 计算机病毒的工作过程

计算机病毒的完整工作过程一般应包括以下几个环节。

(1) 传染源。病毒总是依附于某些如硬盘这样的存储介质，这些存储介质构成传染源。

(2) 传染媒介。病毒传染的媒介由工作环境来决定，可能是计算机网，也可能是可移动的存储介质。

(3) 病毒激活。是指将病毒装入内存，并设置触发条件，触发的条件是多样化的，可以是内部时钟、系统的日期、用户标识符，也可能是系统一次通信等。一旦触发条件成熟，

病毒就开始作用，自我复制到传染对象中，进行各种破坏活动。

(4) 病毒表现。表现是病毒的主要目的之一，有时在屏幕显示出来，有时则表现为破坏系统数据。可以这样说，凡是软件技术能够触发到的地方，都在其表现范围内。

(5) 传染。病毒的传染是病毒性能的一个重要标志。在传染环节中，病毒复制一个自身副本到传染对象中去。

2. 计算机病毒的引导机制

(1) 计算机病毒的寄生对象

计算机病毒存储在磁盘上，为了进行自身的主动传播，必须寄生在可以获得执行权的寄生对象上。就目前出现的各种计算机病毒来看，其寄生对象有两种，一种是寄生在磁盘引导扇区；另一种是寄生在可执行文件(.EXE或.COM)中。不论是磁盘引导扇区还是可执行文件，它们都有获取执行权的可能，病毒程序寄生在它们的上面，就可以在一定条件下获得执行权，从而使病毒得以进入计算机系统，并处于激活状态，然后进行病毒的动态传播和破坏活动。

(2) 计算机病毒的寄生方式

计算机病毒的寄生方式有两种，一种是采用替代法；另一种是采用链接法。所谓替代法，是指病毒程序用自己的部分或全部指令代码，替代磁盘引导扇区或文件中的全部或部分内容。所谓链接法，则是指病毒程序将自身代码作为正常程序的一部分与原有正常程序链接在一起，病毒链接的位置可能在正常程序的首部、尾部或中间，寄生在磁盘引导扇区的病毒一般采取替代法，而寄生在可执行文件中的病毒一般采用链接法。

(3) 驻留内存

计算机病毒若要发挥破坏作用，要开辟所用内存空间或覆盖系统占用的部分内存空间以便驻留内存。当病毒程序驻留内存后，必须使有关部分取代或扩充系统的原有功能，并窃取系统的控制权。此后病毒程序依据其设计思想，隐藏自己，等待时机，在条件成熟时，再进行传染和破坏。

病毒为隐藏自己，驻留内存后还要恢复系统，使系统不会死机，只有这样才能等待时机成熟后，进行感染和破坏的目的。有的病毒在加载之前进行动态反跟踪和病毒体解密。

对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占用了原系统引导程序的位置，并把原系统引导程序转移到一个特定的地方。这样系统一启动，病毒引导模块就会自动地装入内存并获得执行权，然后该引导程序负责将病毒程序的传染模块和发作模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对这两个模块设定某种激活方式，使之在适当的时候获得执行权。这些工作完成后，病毒引导模块装入内存，使系统在带病毒的状态下运行。

对于寄生在可执行文件中的病毒来说，病毒程序一般通过修改原有可执行文件，使该文件执行时首先转入病毒程序引导模块，该引导模块负责把病毒程序的其他两个模块驻留内存及进行初始化的工作，然后把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。

3. 计算机病毒的触发机制

传染、潜伏、可触发、破坏是病毒的基本特性。可触发性是病毒的攻击性和潜伏性之间的调整杠杆，可以控制病毒感染和破坏的频度，兼顾杀伤力和潜伏性。

过于苛刻的触发条件，可能使病毒有好的潜伏性，但不易传播，杀伤力较低。而过于宽松的触发条件将导致病毒频繁感染与破坏，容易暴露，导致用户做反病毒处理，也不能有大的杀伤力。

计算机病毒在传染和发作之前，往往要判断某些特定条件是否满足，满足则传染或发作，否则不传染、不发作或只传染不发作，这个条件就是计算机病毒的触发条件。

实际上病毒采用的触发条件花样繁多，目前病毒采用的触发条件主要有以下几种。

(1) 时间触发。时间触发包括特定的时间触发、染毒后累计工作时间触发、文件最后写入时间触发等。

(2) 键盘触发。有些病毒监视用户的击键动作，当发现病毒预定的输入时，病毒被激活，进行某些特定操作。键盘触发包括击键次数触发、组合键触发、热启动触发等。

(3) 日期触发。许多病毒采用日期作为触发条件。日期触发大体包括特定日期触发、月份触发、前半年后半年触发等。

(4) 启动触发。病毒对机器的启动次数计数，并将此值作为触发条件称为启动触发。

(5) 访问磁盘次数触发。病毒对磁盘 I/O 访问的次数进行计数，以预定次数做触发条件称为访问磁盘次数触发。

(6) 调用中断功能触发。病毒对中断调用次数计数，以预定次数做触发条件。

被计算机病毒使用的触发条件是多种多样的，而且往往不只是使用上面所述的某一个条件，而是使用多个条件组合起来的触发条件。大多数病毒的组合触发条件是基于时间的，再加上读、写操作，按键操作及其他条件。如“侵略者”病毒的激发时间是开机后机器运行时间和病毒传染个数成某个比例时，恰好按 Ctrl+Alt+Del 组合键试图重新启动系统则病毒发作。

病毒中有关触发机制的编码是其敏感部分。剖析病毒时，如果搞清病毒的触发机制，可以修改此部分代码，使病毒失效，就可以产生没有潜伏性的极为外露的病毒样本，供反病毒研究使用。

4. 计算机病毒的破坏行为

计算机病毒的破坏行为体现了病毒的杀伤能力。病毒破坏行为的激烈程度取决于病毒作者的主观愿望和他所具有的技术能量。数以万计、不断发展扩张的病毒，其破坏行为千奇百怪，不可能穷举。我们可以把病毒的破坏目标和攻击部位归纳如下。

(1) 攻击系统数据区。攻击部位包括硬盘主引导区、Boot 扇区、FAT 表、文件目录。一般来说，攻击系统数据区的病毒是恶性病毒，受损的数据不易恢复。

(2) 攻击文件。病毒对文件的攻击方式很多，可列举如下：删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、变碎片、假冒文件、丢失文件簇、丢失数据文件。

（3）攻击内存。内存是计算机的重要资源，也是病毒的攻击目标。病毒额外地占用和消耗系统的内存资源，可以导致一些大程序受阻。病毒攻击内存的方式如下：占用大量内存、改变内存总量、禁止发配内存、蚕食内存。

（4）干扰系统运行。病毒会干扰系统的正常运行，以此作为自己的破坏行为。此类行为也是花样繁多，如不执行命令、干扰内部命令的执行、虚假报警、打不开文件、内部栈溢出、占用特殊数据区、换现行盘、时钟倒转、重启动、死机、强制游戏、扰乱串并口。

（5）运行速度下降。病毒激活时，其内部的时间延迟程序启动。在时钟中纳入了时间的循环计数，迫使计算机空转，计算机速度明显下降。

（6）攻击磁盘。攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节。

（7）攻击 CMOS。在机器的 CMOS 区中，保存着系统的重要数据。如系统时钟、磁盘类型、内存容量等，并具有校验和。有的病毒在激活后，能够对 CMOS 区进行写入动作，破坏系统 CMOS 中的数据。

5. 计算机病毒的传播

（1）计算机病毒传播的一般过程

在系统运行时，计算机病毒通过病毒载体即系统的外存储器进入系统的内存储器，常驻内存。该病毒在系统内存中监视系统的运行，当它发现有攻击的目标存在并满足条件时，便从内存中将自身存入被攻击的目标，从而将病毒进行传播。

（2）计算机病毒的传播途径

计算机病毒具有自我复制和传播的特点，因此，研究计算机病毒的传播途径是极为重要的。从计算机病毒的传播机制分析可知，只要是能够进行数据交换的介质都可能成为计算机病毒传播途径。现在通过 Internet 传播计算机病毒与过去手工传播计算机病毒的方式相比速度要快得多。

目前，网络和电子邮件已经成为最重要的病毒传播途径。

网络是由相互连接的一组计算机组成的，这是数据共享和相互协作的需要。数据能从一台计算机发送到其他计算机上。如果发送的数据感染了计算机病毒，接收方的计算机将自动被感染，因此，有可能在很短的时间内感染整个网络中计算机。

局域网络技术的应用为企业的发展做出了巨大贡献，同时也为计算机病毒的迅速传播创造了条件。特别是 Internet，已经越来越多地被用于获取信息、发送和接收文件、接收和发布新的消息及下载文件的程序。随着 Internet 的高速发展，计算机病毒也走上了高速传播之路，已经成为计算机病毒的第一传播途径。除了传统的文件型计算机病毒以文件下载、电子邮件的附件等形式传播外，电子邮件计算机病毒，如“美丽莎”计算机病毒、“我爱你”计算机病毒等则是完全依靠网络来传播的。甚至还有利用网络分布计算机技术将自身分成若干部分，隐藏在不同的主机上进行传播的计算机病毒。

可移动式磁盘包括 CD-ROM、移动磁盘等，后者仅仅是存储容量比较大的特殊磁盘。盗版光盘上的软件和游戏及非法拷贝是目前传播计算机病毒主要途径之一。随着大容量可移动存储设备的普遍使用，这些存储介质也成为计算机病毒寄生的场所。硬盘是现在数据的主要存储介质，因此，也是计算机病毒感染的重灾区。

计算机病毒也可以通过点对点通信系统和无线通道传播。但目前这种传播途径还不是十分广泛,但预计在未来的信息时代,这种途径很可能与网络传播途径成为病毒扩散的两大途径。

7.1.5 计算机病毒的检测、防范和清杀

随着网络的发展,伴随而来的计算机病毒传播问题越来越引起人们的关注。Internet的普及使有些计算机病毒借助网络爆发流行,如CIH、爱虫、硬盘杀手、好大(I-Worm/Sobig)等病毒,它们与以往的计算机病毒相比具有一些新的特点,给广大计算机用户带来了极大的损失。

在与计算机病毒的对抗中,如果能采取有效的防范措施,就能使系统不染毒,或者染毒后能减少损失。当计算机系统或文件染有计算机病毒时,需要检测和清除。但是,隐性计算机病毒和多态性计算机病毒使人难以检测。

1. 计算机病毒的检测

判断自己的计算机中是否染有病毒,最简单的方法是用较新的防病毒软件对磁盘进行全面的检测。无论什么病毒,在其侵入系统后总会留下一些“蛛丝马迹”。如何能够及早地发现新病毒呢?

常用的检测病毒方法有特征代码法、校验和法、行为监测法、软件模拟法,这些方法依据的原理不同,实现时所需开销不同,检测范围不同,各有所长。

(1) 特征代码法

特征代码法被早期应用于SCAN、CPAV等著名病毒检测工具中。国外专家认为特征代码法是检测已知病毒的最简单、开销最小的方法。

特征代码法的实现步骤如下:采集已知病毒样本,病毒如果既感染.COM文件又感染.EXE文件,对这种病毒要同时采集.COM型病毒样本和.EXE型病毒样本。在病毒样本中,抽取特征代码。

打开被检测文件,在文件中搜索,检查文件中是否含有病毒数据库中的病毒特征代码。如果发现病毒特征代码,由于特征代码与病毒一一对应,便可以断定,被查文件中患有何种病毒。

采用病毒特征代码法的检测工具,面对不断出现的新病毒,必须不断更新版本,否则检测工具便会老化,逐渐失去实用价值。病毒特征代码法对从未见过的新病毒,自然无法知道其特征代码,因而无法去检测这些新病毒。

特征代码法检测准确快速、可识别病毒的名称、误报警率低、依据检测结果,可做解毒处理。但不能检测未知病毒、需搜集已知病毒的特征代码,费用开销大、在网络上效率低(在网络服务器上,因长时间检索会使整个网络性能降低)是它的缺点。

(2) 校验和法

计算正常文件内容的校验和,将该校验和写入文件中或写入别的文件中保存。在文件使用过程中,定期地或每次使用文件前,检查文件现在内容算出的校验和与原来保存的

校验和是否一致，因而可以发现文件是否感染，这种方法叫校验和法，它既可发现已知病毒又可发现未知病毒。

校验和法方法较简单，能发现未知病毒，即使被查文件发生细微变化也能发现，但发布通行记录正常态的校验和、误报警、不能识别病毒名称、不能对付隐蔽型病毒是它的缺点。

(3) 行为监测法

行为监测法是指利用病毒的特有行为特征性来监测病毒的方法。病毒有一些共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为，如果发现了病毒行为，则立即报警。

行为监测法可以发现未知病毒，可相当准确地预报未知的多数病毒。可能误报警、不能识别病毒名称、实现时有一定难度是它的缺点。

2. 计算机病毒的防范

防范是对付计算机病毒的积极而有效的措施，相比等待计算机病毒出现之后再去扫描和清除能更有效地保护计算机系统。要做好计算机病毒的防范工作，首先是防范体系和制度的建立；其次，利用反病毒软件及时发现计算机病毒侵入，对它进行监视、跟踪等操作，并采取有效的手段阻止它的传播和破坏。

老一代的反病毒软件只能对计算机系统提供有限的保护，只能识别已知的计算机病毒。新一代的反病毒软件则不仅能识别出已知的计算机病毒，在计算机病毒运行之前发出警报，还能屏蔽掉计算机病毒程序的传染功能和破坏功能，使受感染的程序可以继续运行(即所谓的带毒运行)。同时还能利用计算机病毒的行为特征，防范未知计算机病毒的侵扰和破坏。另外，新一代的反病毒软件还能实现超前防御，将系统中可能被计算机病毒利用的资源都加以保护，不给计算机病毒以可乘之机。

计算机病毒的工作方式是可以分类的，反病毒软件就是针对已归纳总结出的这几类计算机病毒工作方式来进行防范的。当被分析过的已知计算机病毒出现时，由于其工作方式早已被记录在案，反病毒软件能识别出来；当未曾被分析过的计算机病毒出现时，如果其工作方式仍可被归入已知的工作方式，则这种计算机病毒能被反病毒软件所捕获。这也就是采取积极防御措施的计算机病毒防范方法优越于传统方法的地方。

当然，如果新出现的计算机病毒不按已知的方式工作，这种新的传染方式又不能被反病毒软件所识别，那么反病毒软件也无能为力了。

这时只能采取两种措施进行保护：第一是依靠管理上的措施，及早发现疫情，捕捉计算机病毒，修复系统；第二是选用功能更加完善的、具有更强超前防御能力的反病毒软件，尽可能多地堵住能被计算机病毒利用的系统漏洞。

反病毒软件常用以下几种反病毒技术来对病毒进行预防和彻底杀除。

(1) 实时监视技术

实时监视技术为计算机构筑起一道动态、实时的反病毒防线，通过修改操作系统，使操作系统本身具备反病毒功能。时刻监视系统当中的病毒活动、系统状况，时刻监视软盘、光盘、Internet、电子邮件上的病毒传染，将病毒阻止在操作系统外部。优秀的反病毒

软件由于采用了与操作系统的底层无缝连接技术，实时监视器占用的系统资源极小，用户一方面完全感觉不到对机器性能的影响；另一方面根本不用考虑病毒的问题。

只要实时反病毒软件实时地在系统中工作，病毒就无法侵入我们的计算机系统。可以保证一旦安装反病毒软件，计算机运行的每一秒钟都会执行严格的反病毒检查。

（2）全平台反病毒技术

目前病毒活跃的平台有 Windows XP/2003/2008/等。为了反病毒软件做到与系统的底层无缝连接，可靠地实时检查和杀除病毒，必须在不同的操作系统平台上使用相应平台的反病毒软件，如用的是 Windows 的平台，则必须用 Windows 版本的反毒软件。如果是企业网络，什么版本的平台都有，那么就要在网络的每一个服务器端和客户端上安装相应平台的反病毒软件，每一个点上都安装相应的反病毒模块，每一个点上都能实时地抵御病毒攻击。只有这样，才能做到网络的真正安全和可靠。

7.2 网络病毒的防范和清除

网络病毒通过计算机网络传播感染网络中的可执行文件，它的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大。

1. 网络病毒的防范措施

相对于单机病毒的防护来说网络病毒的防范具有更大的难度，网络病毒的防范应与网络管理集成。网络防毒的最大优势在于网络的管理功能，如果没有把管理功能加上，很难完成网络防毒的任务，只有管理与防范相结合，才能保证系统的良好运行。管理功能就是管理全部的网络设备与操作；从 HUB、交换机、服务器到个人计算机，包括硬盘的存取、局域网上的信息互通与 Internet 的接驳等所有病毒能够感染和传播的途径。

在网络环境下，病毒传播扩散快，仅用单机反病毒产品已经难以清除网络病毒，必须有适用于局域网、广域网的全方位反病毒产品。

在选用反病毒软件时，应选择对病毒具有实时监控能力的软件，这类软件可以在第一时间阻止病毒感染，而不是靠事后去杀毒。要养成定期升级防病毒软件的习惯，并且间隔时间不要太长，因为绝大部分反病毒软件的查毒技术都是基于病毒特征码的，即通过对已知病毒提取其特征码，并以此来查杀同种病毒。对于每天都可能出现的新病毒，反病毒软件会不断更新其特征码数据库。

要养成定期扫描文件系统的习惯；对移动存储介质，在使用之前应进行查毒；对于从网上下载的文件和电子邮件附件中的文件，在打开之前也要先杀毒。另外，由于防病毒软件总是滞后于病毒的，因此它通常不能发现一些新的病毒。因此，不能只依靠防病毒软件来保护系统。在使用计算机时，还应当注意以下几点。

（1）不使用或下载来源不明的软件。

（2）不轻易浏览一些不正规的网站。

（3）提防电子邮件病毒的传播。一些邮件病毒会利用 ActiveX 控件技术，当以 HTML 方式打开邮件时，病毒可能就会被激活。

(4) 经常关注一些网站、BBS 发布的病毒报告,这样可以在未感染病毒时做到预先防范。

(5) 及时更新操作系统,为系统漏洞打上补丁。

(6) 对于重要文件、数据做到定期备份。

2. 网络病毒的清杀

一旦在网络上发现病毒,应设法立即清除,其操作步骤如下。

(1) 立即通知所有用户下网,关闭文件服务器。

(2) 用带有写保护的、干净的系统盘启动系统管理员工作站,并立即清除本机病毒。

(3) 用带有写保护的、干净的系统盘启动文件服务器。系统管理员登录并下命令禁止其他用户登录。

(4) 将文件服务器硬盘中的重要资料备份。但严禁执行硬盘上的程序和在硬盘中拷贝文件,以免破坏被病毒搞乱的硬盘数据结构。

(5) 用杀毒软件扫描服务器上所有的文件,恢复或删除被病毒感染的文件,重新安装被删除的文件。

(6) 用杀毒软件扫描并清除所有可能染上病毒的磁盘或备份文件中的病毒。

(7) 用杀毒软件扫描并清除所有有盘工作站硬盘上的病毒。

(8) 在确信病毒已经彻底清除后,重新启动网络和工作站。

7.3　典型的网络病毒

7.3.1　宏病毒

1. 宏病毒的定义

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档,其中的宏就会被执行,于是宏病毒就会被激活而转移到计算机上,并驻留在 Normal 模板上。从此以后,所有自动保存的文档都会感染上这种宏病毒,而且如果其他用户打开了感染病毒的文档,宏病毒就会转移到他的计算机上。如果某个文档中包含了宏病毒,此文档就是感染了宏病毒;如果 Word 文档中的模板包含了宏病毒,就可以认为 Word 感染了宏病毒。

所谓宏,就是软件设计者为了在使用软件工作时,避免一再地重复相同的动作而设计出来的一种工具。它利用简单的语法,把常用的动作写成宏,当再工作时,就可以直接利用事先写好的宏自动运行,去完成某项特定的任务,而不必再重复相同的动作。Word 中把宏定义为“宏就是能组织到一起作为一独立的命令使用的一系列 Word 命令,它能使日常工作变得更容易。”Word 宏就是使用 Word Basic 语言来编写的。“宏病毒”就是利用软件所支持的宏命令编写的具有复制、传染能力的宏。

2. 宏病毒的特征

计算机病毒具有以下特征。

(1) 宏病毒会感染.doc文档和.dot模板文件。

(2) 宏病毒的传染通常是Word在打开一个带宏病毒的文档或模板时,激活宏病毒,病毒宏将自身复制到Word通用(Normal)模板中,以后在打开或关闭文件时宏病毒就会把病毒复制到该文件中。

(3) 多数宏病毒包含AutoOpen、AutoClose、AutoNew和AutoExit等自动宏,通过这些自动宏病毒取得文档(模板)操作权。

(4) 宏病毒中总是含有对文档读/写操作的宏命令。

(5) 宏病毒在.doc文档和.dot模板中以BFF(binary file format)格式存放,这是一种加密压缩格式,不同Word版本格式可能不兼容。

(6) Word宏病毒在发作时,会使Word运行出现怪现象,如自动建文件、开窗口、内存总是不够、关闭Word并不对已修改文件提出未存盘警告、存盘文件丢失等,有的使打印机无法正常打印。Word宏病毒在传染时,会使原有文件属性和类型发生改变,或Word自动对磁盘进行操作等。当内存中有Word宏病毒时,原Word文档无法另存为其他格式的文件,只能以模板形成进行存储。

3. 宏病毒的防范和清除

宏病毒的防治和清除方法如下。

(1) 使用选项"提示保存Normal模板"。

(2) 不要通过Shift键来禁止运行自动宏。

(3) 查看宏代码并删除。

(4) 使用Disable Auto Macros宏。

(5) 设置Normal.dot的只读属性。

(6) Normal.dot的密码保护。

7.3.2 电子邮件病毒

风靡全球的"美丽莎"、Papa和HAPPY 99等计算机病毒正是通过电子邮件的方式进行传播、扩散的,其结果是导致邮件服务器瘫痪、用户信息和重要文档泄密,无法收发电子邮件,给个人、企业和政府部门造成严重的损失。为此有必要介绍一下电子邮件病毒。

电子邮件病毒实际上并不是一类单独的计算机病毒,严格地说它应该划入文件型计算机病毒及宏病毒中去,只不过由于这些病毒采用了独特的电子邮件传播方式(其中不少种类还专门针对电子邮件的传播方式进行了优化),因此,我们习惯于将它们称为电子邮件病毒。

所谓电子邮件病毒,就是以电子邮件作为传播途径的计算机病毒,实际上该类病毒和普通的病毒一样,只不过是传播方式改变而已。该类计算机病毒的特点包括以下几方面。

(1) 电子邮件本身是无毒的,但它的内容中可以有UNIX下的特殊的换码序列,就是

通常所说的 ANSI 字符，当用 UNIX 智能终端上网查看电子邮件时，有被侵入的可能。

(2) 电子邮件可以夹带任何类型的文件作为附件，附件文件可能带有病毒。

(3) 可利用某些电子邮件收发器特有的扩充功能，如 Outlook/Outlook Express 能够执行 VBA 指令编写的宏，在电子邮件中夹带有针对性的代码，利用电子邮件进行传染、扩散。

(4) 超大的电子邮件或电子邮件炸弹也可以被认为是一种电子邮件计算机病毒，它能够影响邮件服务器的正常服务功能。

通常对付电子邮件计算机病毒，只要删除携带电子邮件病毒的信件就能够删除它。但是大多数的电子邮件计算机病毒一被接收到客户端时就开始发作了，基本上没有潜伏期。所以预防电子邮件病毒是至关重要的。以下是一些常用的预防电子邮件病毒的方法。

(1) 及时下载安装操作系统的漏洞补丁程序，同时也要关注热门第三方应用软件的漏洞更新。

(2) 及时升级计算机系统中防病毒软件和防火墙。

(3) 不要随意点击或运行通过 QQ、MSN、电子邮件发来的陌生链接地址或文件。

(4) 提高自己私密性数据的安全，最好经常更换或是设置比较复杂的账户密码。

对付电子邮件计算机病毒，还可以在计算机上安装有电子邮件实时监控功能的防杀计算机病毒软件。有条件的还可以在电子邮件服务器上安装服务器版电子邮件计算机病毒防护软件，从外部切断电子邮件计算机病毒的入侵途径，确保整个网络的安全。

7.3.3　网络病毒实例

1. 电子邮件炸弹

电子邮件炸弹是指发件者以不明来历的电子邮件地址，不断重复将电子邮件寄于同一个人。由于情况就像是战争时利用某种战争工具对同一个地方进行大轰炸，因此称为电子邮件炸弹。

电子邮件炸弹之所以可怕，是因为它可以大量消耗网络资源。一般网络用户电子邮箱的容量都是有限的，如果在短时间内收到上千个电子邮件，而每个电子邮件又占据了一定的容量，一个电子邮件炸弹的总容量很容易就超过用户的电子邮箱所能够承受的负荷。在这样的情况下，用户的电子邮箱不仅不能再接收其他人寄来的电子邮件，也随时会因为“超载”而导致整个计算机瘫痪。

没有人知道自己什么时候会碰到电子邮件炸弹，所以采取防范措施是必要的，比较有效的防御方式是，用户可以在电子邮件中安装一个过滤器，在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，可以将它删除，不让它进入电子邮箱。

2. 恶意网页

(1) 恶意网页的原理

对于恶意网页，常常采取 VBScript 和 JavaScript 编程的形式，由于编程方式十分简单，所以在网上非常流行。VBScript 和 JavaScript 是由微软操作系统的 WSH(Windows

scripting host,Windows 脚本主机)解析并执行的,由于其编程非常简单,所以此类脚本病毒在网上疯狂传播,疯狂一时的“爱虫”病毒就是一种脚本病毒,然后伪装成邮件附件诱惑用户点击运行,更为可怕的是,这样的病毒是以源代码的形式出现的,只要懂得一点关于脚本编程的人就可以修改其代码,形成各种各样的变种。

```
Set objFs=CreateObject
("Scripting.FileSystem Object")(创建一个文件系统对象)
objFs.CreateTextFile("C:\simple.txt",1)
(通过文件系统对象的方法创建了 TXT 文件)
```

如果我们把这句话保存为.vbs 的 VB 脚本文件,单击它就会在 C 盘创建一个 TXT 文件。

倘若我们把第三行改为:objFs.GetFile(Wscript.ScriptFullName)Copy(“C:\simple.vbs”)就可以将自身复制到 C 盘 simple.vbs 这个文件中。本句前面是打开这个脚本文件,Wscript.ScriptFullName 指明是这个程序本身,是一个完整的路径文件名。GetFile 函数获得这个文件,Copy 函数将这个文件复制到 C 盘根目录下 simple.vbs 这个文件中。这么简单的两句代码就实现了自我复制的功能,它已经具备病毒的基本特征——自我复制能力。

此类病毒往往是通过邮件传播的,在 VBScript 中调用邮件发送功能也非常简单,病毒往往采用的方法是向 Outlook 的地址簿中的邮件地址发送带有包含自身的邮件来达到传播的目的,此类病毒的变种繁多,破坏力极大,同时也是非常难以根除的。

(2)恶意网页的预防

① 禁用 WindowsScriptingHost(WSH)。WSH 运行各种类型的文本,但基本都是 VBScript 或 JavaScript。WSH 在文本语言之间充当翻译的角色,该语言可能支持 ActiveXScripting 界面,包括 VBScript、JavaScript、Perl 及所有 Windows 的功能,包括访问文件夹、文件快捷方式、网络接入和 Windows 注册等。许多病毒或蠕虫就是使用 WSH。具体方案是:在 IE 窗口中选择“工具”→“Internet 选项”命令,在弹出的对话框中选择“安全”选项卡,再单击“自定义级别”按钮,就会弹出“安全设置”对话框,把其中所有 ActiveX 插件和控件及与 Java 相关全部选项选择“禁用”。但是,这样做在以后的网页浏览过程中有可能会使一些正常应用 ActiveX 的网站无法浏览。

② 不要轻易去点击陌生的站点,网站里面有可能就含有恶意代码。因为这一类网页含有的恶意代码主要是 ActiveX 或 Applet、JavaScript 文件,所以在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止就可以大大减少被网页恶意代码感染的几率。当运行 IE 时,选择“工具”→“Internet 选项”命令,在出现的对话框中选择“安全”选项卡,在“Internet 区域的安全级别”中把安全级别由“中”改为“高”。

③ 不随意查看陌生邮件,尤其是带有附件的邮件。因为 Windows 允许文件名使用多个后缀,而电子邮件一般只显示第一个后缀,如.jpg,该文件可能是.jpg.vbs,打开这个文件可能意味着运行一个恶意的 VBScript 病毒,而不是.jpg 文件。病毒邮件能够利用 IE 和 Outlook 的漏洞自动执行,所以计算机用户需要升级 IE 和 Outlook 程序及常用的

其他应用程序。

④ 安装防病毒产品并保证更新最新的病毒特征码。首次安装病毒软件时，一定要对机器做一次彻底扫描，以确保它未受到过病毒的感染，用户应当及时更新病毒库。


【案例】“蠕虫”病毒的防范

案例分析

1. 病毒描述

Worm. Win32. Fujack. x 为蠕虫类病毒，病毒运行后复制自身到系统目录，衍生病毒文件、修改注册表、添加启动项，以达到随机启动的目的，并删除安全相关服务，减弱系统安全性。该病毒具有多种启动方式，而且具有修改注册表隐藏自身的功能。所以此病毒用常规方法很难清除，生存期会相对较长。该病毒对用户的计算机信息具有严重的威胁。

2. 行为分析

(1) 文件运行后会衍生以下文件。

```
%DriveLetter%\autorun.inf
%DriveLetter%\setup.exe
%WinDir%\SchedLgU.Txt
%System32%\drivers\spoclss.exe
%WinDir%\Tasks\SA.DAT
```

(2) 新建注册表如下。

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
```

注册表值："svcshare"。

类型：REG_SZ。

值："C:\WINDOWS\system32\drivers\spoclss.exe"。

描述：添加启动项，以达到随机启动的目的。

(3) 修改注册表如下。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue]
```

新：DWORD：0 (0)。

旧：DWORD：1 (0x1)。

描述：使隐藏文件不可见。

(4) 删除安全相关服务。

服务名称：wscsvc。

显示名称：Security Center。

描述语言：监视系统安全设置和配置。

文件路径：%SystemRoot%\System32\svchost.exe -k netsvcs。

启动方式：自动。

(5) 在各个驱动器盘符下释放启动文件 autorun.inf 和与其对应的执行文件 setup.exe，autorun.inf 的内容如下。

```
[AutoRun]
OPEN=setup.exe
shellexecute=setup.exe
shell\Auto\command=setup.exe
```

(6) 将自身添加到 Tasks 文件夹下的计划任务中，任务计划的相关信息在 SchedLgU.Txt 内记录。

操作环境

(1) 连上 Internet 的主机或局域网主机。

(2) Windows Server 2003、Windows XP 系统。

操作步骤

第 1 步 使用最新杀毒软件或木马专杀软件可彻底清除此病毒。

第 2 步 手工清除请按照行为分析删除对应文件，恢复相关系统的设置。

(1) 在“进程管理”中关闭病毒进程。

(2) 强行删除下面病毒文件。

```
%DriveLetter%\autorun.inf
%DriveLetter%\setup.exe
%WinDir%\SchedLgU.Txt
%System32%\drivers\spoclss.exe
%WinDir%\Tasks\SA.DAT
```

(3) 恢复病毒修改的注册表项目，删除病毒添加的注册表项。

① 删除新建注册表。

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
```

注册表值为"svcshare"，类型为“REG_SZ”。

值："C:\WINDOWS\system32\drivers\spoclss.exe"。

描述：添加启动项，以达到随机启动的目的。

② 恢复修改注册表。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL\CheckedValue]
```

新：DWORD：0 (0)。

旧：DWORD：1 (0x1)。

描述：使隐藏文件不可见。

7.4　常用的杀毒软件

随着世界范围内计算机病毒的大量流行，新的病毒不断出现，各种反病毒软件产品也在不断地推陈出新、更新换代。这些产品的特点表现为技术领先、误报率低、杀毒效果明显、界面友好、具有良好的升级和售后服务技术支持、与各种软/硬件平台兼容性好等方面。国内常用的反病毒软件有瑞星杀毒软件 2012、金山杀毒软件、诺顿 2012、360 杀毒软件等。

7.4.1　瑞星杀毒软件

瑞星杀毒软件 2012 是北京瑞星科技股份有限公司采用最新技术开发的新一代信息安全产品。

瑞星杀毒软件 2012 以瑞星最新研发的变频杀毒引擎为核心，通过变频技术使计算机得到安全保证的同时，又大大降低资源占用，让计算机更加轻便。同时，瑞星 2012 版应用"瑞星云安全+"技术、"云查杀"、"网购保护"、"智能、安全上网"和智能反钓鱼等技术，保护网购、网游、微博、办公等常见应用面临的各种安全问题，通过友善易用的界面和更小的资源占用为用户提供全新安全软件体验。

瑞星杀毒软件 2012 的具体功能如下。

(1) 瑞星变频杀毒技术。智能检测计算机资源占用，自动分配杀毒时占用的系统资源，既保障计算机的正常使用，又保证计算机的安全。

(2) 瑞星"云查杀"。大大降低用户计算机资源的占用，杀毒速度快速提升，无须升级即可查杀最新病毒。

(3) 网购保护。在用户进行网上购物、支付、访问网银等操作时自动进行保护，防止黑客、木马病毒等问题对用户网上银行财产产生威胁，确保网购安全。

(4) 智能、安全上网。通过"智能反钓鱼"、"安全搜索"、"木马下载拦截"、"家长控制"、"ADSL 带宽管家"等大量新增功能，保证用户安全上网、绿色上网、智能上网。

(5) 体积小、资源小、高效升级。安装包体积小、杀毒速度快速提升、对系统影响小，升级时只下载几千字节的文件，减小带宽占用。



【案例】　使用瑞星杀毒软件对计算机病毒进行检测与防范

案例分析

杀毒软件通常集成监控识别、病毒扫描和清除和自动升级等功能，是计算机防御系统(包含杀毒软件、防火墙、特洛伊木马和其他恶意软件的查杀程序、入侵预防系统等)的重要组成部分。

操作环境

(1) 连上 Internet 的 Windows Server 2003、Windows XP 系统主机一台。

(2) 瑞星杀毒软件 2012。

操作步骤

第 1 步 安装瑞星杀毒软件(个人版)。

第 2 步 了解瑞星杀毒软件的操作界面。

如图 7.1 所示,从瑞星杀毒软件界面的菜单栏中可以看到杀毒、电脑防护、瑞星工具和安全资讯 4 个选项卡。其中"杀毒"选项卡中包含有快速查杀、全盘查杀、自定义查杀;"电脑防护"选项卡主要是对文件监控,包括邮件监控、U 盘防护、木马防御、浏览器保护、办公软件保护、系统内核加固;"瑞星工具"选项卡包括卡卡上网安全助手、瑞星助手、引导区还原、瑞星安装包制作、账号保险柜、病毒库 U 盘备份、Linux 引导盘制作等子菜单栏;"安全资讯"选项卡提供最新资讯。



图 7.1 瑞星杀毒软件操作界面

第 3 步 使用瑞星杀毒软件。

(1) 设置。先单击"设置"按钮,进入"设置"界面,从中可以对查杀的方式和级别进行设置,如图 7.2 所示。

(2) 查毒、清除杀毒软件发现的病毒。进入"杀毒"选项卡,搜索系统中是否存在病毒,若发现,就清除掉,如图 7.3 所示。

第 4 步 文件监控。

在"电脑防护"选项卡可对要防护和监控的对象进行设置,以实现对计算机文件的监控,如图 7.4 所示。

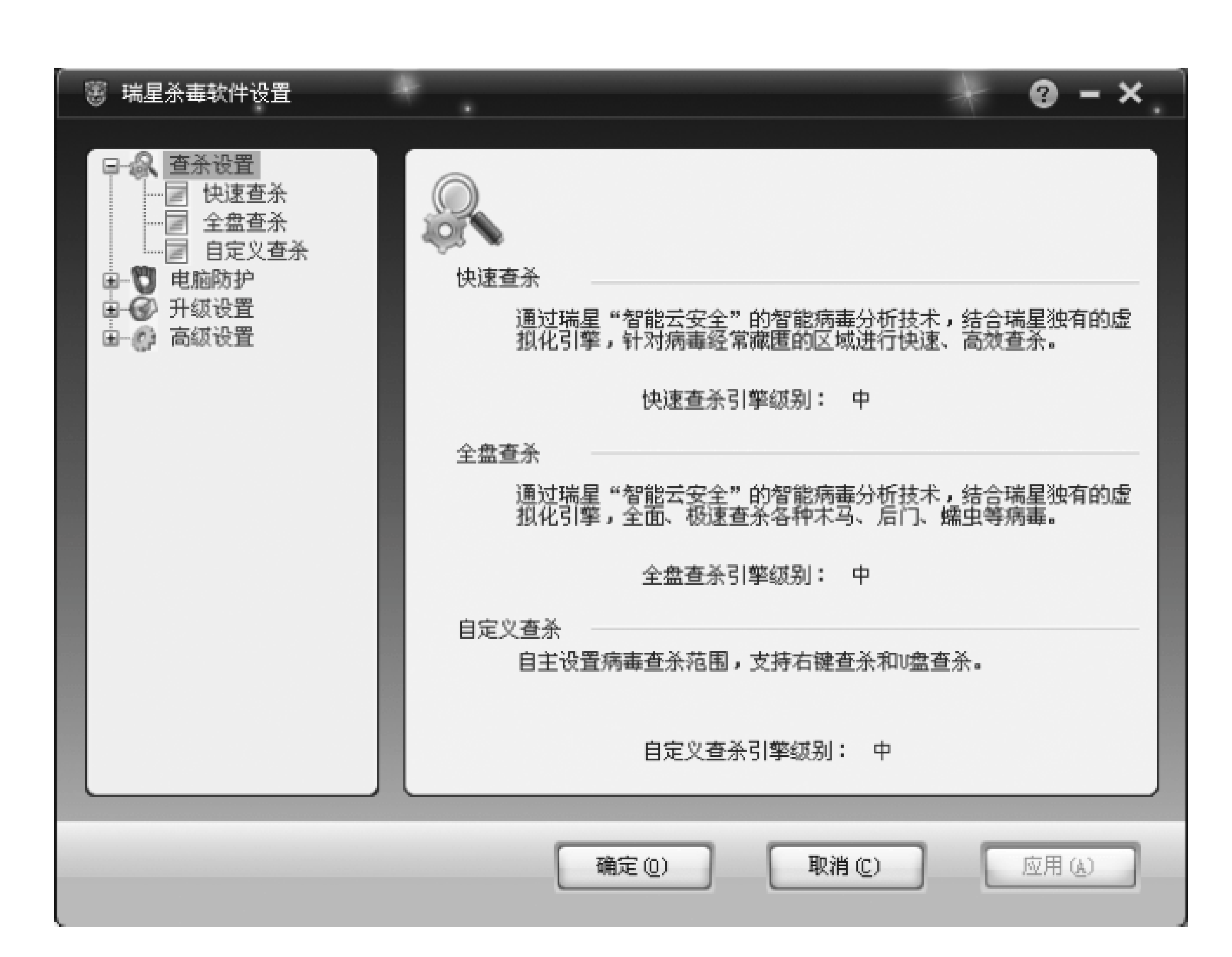


图 7.2　"设置"界面



图 7.3　"杀毒"选项卡



图 7.4　"电脑防护"选项卡

第 5 步 升级瑞星杀毒软件。

在瑞星杀毒软件的主界面中，单击“软件升级”按钮，可以将瑞星杀毒软件升级到最新版，如图 7.5 所示。

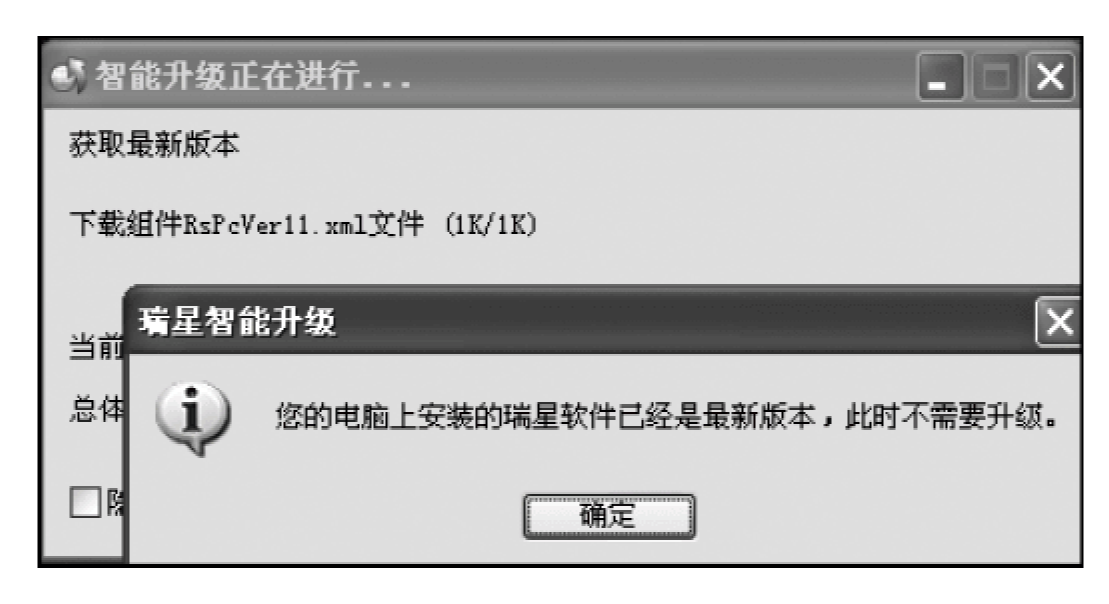


图 7.5 软件升级

7.4.2 金山杀毒软件

金山公司是国内著名的软件公司，其开发的金山毒霸对查毒速度进行了优化，可以快速、彻底地查杀多种流行病毒。

金山毒霸 2012 极速轻巧，安装包不到 20MB，内存占用只有 19MB，首次扫描仅 4 分钟，3 分钟消灭活木马，扫描速度每秒可达 134 个文件。配合中国互联网最大云安全体系，100%鉴定文件是病毒还是正常文件。强大的自动分析鉴定体系可在 60 秒钟内鉴定 Internet 上 95%的未知文件，应用精确样本收集技术更使文件鉴定准确率达到了 99%以上。

金山毒霸 2012 技术亮点如下。

(1) 可信云查杀。增强 Internet 可信认证，海量样本自动分析鉴定，极速快速匹配查询。

(2) 蓝芯Ⅱ云引擎(BlueChipⅡCLOUD)。微特征识别(启发式查杀 2.0)，将新病毒扼杀于摇篮中，针对类型病毒具有不同的算法，减少资源占用，多模式快速扫描匹配技术，超快样本匹配。

(3) 白名单优先技术。准确标记用户计算机所有安全文件，无须逐一比对病毒库，大大提高效率，双库双引擎，首家在杀毒软件中内置安全文件库，与可信云安全紧密结合，安全少误杀。

(4) 个性功能体验。下载保护、聊天软件保护、U 盘病毒免疫防御、文件粉碎机、自定义安全区，提升性能、可定制的免打扰模式、自动调节资源占用、针对笔记本电源优化使续航更久。

7.4.3 诺顿杀毒软件

诺顿反病毒产品包括诺顿网络安全特警(Norton Internet Security)、诺顿反病毒(Norton Antivirus)、诺顿 360(Norton ALL-IN-ONE Security)、诺顿计算机大师(Norton SystemWorks)等产品。还有一种专供企业使用的版本被称为 Symantec Endpoint Protection。

1. 诺顿杀毒产品的优势

(1) 严密防范黑客、病毒、木马、间谍软件和蠕虫等攻击。

(2) 动态仿真反病毒专家系统分析识别出未知病毒后，能够自动提取该病毒的特征值，自动升级本地病毒特征值库，实现对未知病毒捕获、分析、升级的智能化。

(3) 驱动级安全保护机制，避免自身被病毒破坏而丧失对计算机系统的保护作用。

(4) 即使在 Windows 系统漏洞未进行修复的情况下，依然能够有效检测到黑客利用漏洞进行的溢出攻击和入侵，实时保护计算机的安全。避免因为用户因不便安装系统补丁而带来的安全隐患。

(5) 拦截远程攻击时，同步准确记录远程计算机的 IP 地址，协助用户迅速、确定攻击源，并能够提供攻击计算机准确的地理位置，实现攻击源的全球定位。

2. 诺顿 2012 版新特性

新版安全软件新增诺顿 360 年初首次添加的启动管理器，并改进了 Sonar 主动防护技术。

Chrome 浏览器支持是诺顿用户一直所期待的功能，Norton Safe Web(诺顿网页安全检测)工具栏现在可以为 Chrome 用户提供搜索结果评估，链接扫描和用户身份认证等功能。

诺顿 2012 测试版对病毒扫描引擎进行了两处改进，但用户界面模块变化很小。Insight 3.0(智能扫描)及其组件 Download Insight 2.0(下载智能分析)都得以改进。Download Insight 功能可以监测下载文件，以保证文件安全性和稳定性。尽管 Download Insight 还是无法阻止用户下载已知威胁文件，但它会提供一个停止下载选项。

Download Insight 是一项精心设计的功能，它还针对不同的系统进行了设计。如果一个文件在 Windows 7 环境下安全但在 Windows XP 环境下不安全，只有 Windows XP 用户会看到停止下载提示。

同时，Sonar 4.0 还升级了行为防护功能，监测可疑程序的运行，并且可在适当的时候停止程序运行。另外，Sonar 现在还可以逐个评定 DLL 文件，以方便详细地监测。

当然，诺顿 2012 测试版也对界面进行了细微的改变，在传统的黄黑界面添加了亮绿色。诺顿在线存储服务也有一些改进，如整合了云同步功能。诺顿启动恢复工具还新增了 Norton Power Eraser(诺顿恶意软件清理工具)，用户无须分别安装这些工具。

本章小结

计算机病毒指编制或者在计算机程序中插入的破坏计算机功能数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码，具有传染性、潜伏性、触发性和破坏性。计算机病毒可归纳为引导型病毒、可执行病毒、宏病毒、混合型病毒、特洛伊木马病毒和网页病毒 6 种类型。

计算机网络病毒具有高频度、传播速度快、危害面广、制作技术新、形式多样化和病毒

生成工具比较易得等特点。

最后简单介绍了网络病毒的检测、防范和清杀方法及常用反病毒软件，如瑞星杀毒软件 2012、金山毒霸 2012 和诺顿 2012。

本章练习

一、填空题

1. 计算机病毒的特征包括________、________、________、________。
2. 计算机病毒可分为________、________、________、________、________和________ 6 种类型。
3. 按照计算机病毒的传播媒介来分类，可分为________病毒和________病毒。
4. 网络反病毒技术主要有 3 种，它们是预防病毒技术、________病毒技术和清除病毒技术。
5. 电子邮件炸弹是________。

二、选择题

1. 计算机病毒是________。
   A. 一种程序　　B. 传染病病毒
   C. 一种计算机硬件　　D. 计算机系统软件
2. 下列不属于计算机病毒特性的是________。
   A. 传染性　　B. 突发性　　C. 可预见性　　D. 隐藏性
3. 计算机病毒________。
   A. 都具有破坏性　　B. 有些无破坏性
   C. 都破坏. exe 文件　　D. 不破坏数据，只破坏文件
4. 计算机病毒________。
   A. 是生产计算机硬件时不注意产生的　　B. 都是人为制造的
   C. 都必须清除计算机才能使用　　D. 有可能是人们无意中制造的
5. 计算机病毒________。
   A. 破坏都是巨大的　　B. 都具有可知性
   C. 只破坏计算机软件　　D. 是可预防的

三、简答题

1. 什么是计算机病毒？
2. 计算机病毒的基本特征是什么？
3. 计算机病毒可以分为哪几类？
4. 简述网络病毒的清除方法。
5. 计算机网络病毒的预防有哪几个方面？
6. 简述计算机网络病毒的防治措施。

实训　U 盘病毒的工作原理及清除方法

实训目的

（1）了解 U 盘病毒的工作原理。
（2）掌握 U 盘病毒的清除方法

实训环境

Windows 操作系统，U 盘，计算机内已安装的其他程序。

实训原理

一些病毒程序独立存放在移动存储设备中，并建立移动盘自动启用文件，当使用者打开移动存储设备时，自动启用文件引导病毒程序。

自动启用文件是微软公司为了方便用户启动程序而设置的一种名为 autorun.inf 的文本文件，位于移动盘的根目录，以纯文本的方式存放各种控制命令，用户双击盘符打开盘时就会自动打开并执行里面的命令。

如果自动启动文件被病毒所利用，当用户双击打开移动盘时就会自动启动病毒程序。

实训步骤

第 1 步　使用记事本或其他文本编辑软件在 U 盘中建立名为 autorun.inf 的文本文件。

文件内容如下。

```
[autorun]  这是自动启动文件固定格式.
Shellexecute=c:\windows\system32\calc.exe;也可以是其他可执行程序或文档;下面内容不是必需的,是病毒采取的隐藏或迷惑用户的常用手法.
icon=calc.exe  更改移动盘图标为计算器.
Label  计算器,更改移动盘图标为计算器.
Shell\计算器\Command=c:\windows\system32\calc.exe;在快捷菜单中添加计算器命令.
```

第 2 步　将上述文本文件以 autorun.inf 为文件名保存到 U 盘根目录。

第 3 步　重新插入 U 盘。

第 4 步　计算器自动启动。

第 5 步　U 盘病毒的清除方法。

方法 1：删除 autorun.inf 文件。

方法 2：格式化 U 盘。

第 8 章

网络攻防技术

Chapter 8

知识目标

- 了解黑客的概念、黑客的攻击目的。
- 了解黑客常用的攻击方法。
- 了解黑客常用攻击工具,面对攻击知道如何防范。

技能目标

- 掌握常见“木马”攻击与防范方法。
- 掌握黑客常用攻击工具及攻击的防范应用。
- 能对网络服务器进行安全配置。

黑客是指未经许可,闯入他人计算机系统的任何人。了解黑客的行为及攻击的方法,可以使我们加强网络安全的意识。黑客技术的发展,使网络安全成为网络设计与维护的重要内容,同时也促进了防范技术的发展。

8.1 黑客的定义

在网络世界里,可以把黑客定义为那些利用计算机技术及其他手段,恶意或善意地进入非授权范围内的计算机或网络空间的人。

目前,黑客的特征主要表现在以下几个方面。

1. 黑客群体扩大化

越来越多的人尤其是年轻人热衷于黑客技术。由于计算机和网络技术的普及,一大批没有受过系统计算机和网络技术教育的黑客人才涌现出来。黑客群体中的绝大多数人是由好奇心驱使的,这类黑客掌握较少的技术,使用现成的工具,攻击不设防的系统。少部分的黑客自己编写工具进行攻击,这部分黑客掌握着较好的技术,能够进入有所防备的系统,但是在一般情况下,他们有自己的道德观念和伦理文化,基本上不会有意破坏他人的系统和数据。还有极少数被称为间谍的黑客,这类黑客是执著的进攻者,他们或因经济利益的关系,或因政治的原因,利用所掌握的技术或工具干扰被攻击系统的正常工作。

2. 黑客的组织化和集团化

目前，以前的那种以个人行为为主的黑客越来越少，被取而代之的是大批黑客组织。黑客组织化和集团化的优势是利用成员各自的不同特长进行合作攻击，从而提高攻击的成功率。

3. 黑客行为的商业化

大多数黑客把技术当成谋生的手段。这些人一般在与网络技术相关的公司里工作，依靠自己高超的计算机和网络技术来设计、研制和管理安全产品。

4. 黑客行为的政治化

由于网络在人们的生产生活，尤其是国家军事安全中占有越来越重要的地位，致使网络完全可能会直接影响到国家安全。因此，各国政府都在准备迎接未来信息战争的挑战。相当多的黑客被政府部门雇用，去从事国家网络安全与攻击的研究。

8.2　黑客攻击的目的和步骤

1. 黑客攻击的目的

一般情况下，黑客的攻击总有明确的目的性。由于黑客成长的经历和生活环境不同，其攻击目标也会多种多样，但大致上可以归纳总结如下。

(1) 窃取信息

黑客攻击最直接的目标就是窃取信息。黑客选取的攻击目标往往是许多重要的信息和数据，在获得这些信息与数据之后，黑客就可以进行各种犯罪活动。政府、军事、邮电和金融网络是黑客攻击的首选目标。随着计算机与网络技术在政府、军事、金融、医疗、交通及电子等各个领域的广泛应用，黑客的各种破坏活动也随之猖獗。

窃取信息包括破坏信息的保密性和完整性。破坏信息的保密性是指黑客将窃取到的需要保密的信息发往公开的站点。而破坏信息的完整性是指黑客对重要文件进行修改、更换和删除，使原来的信息发生了变化，以至于不真实或者错误的信息给用户带来难以估量的损失。

事实上，获取口令也是窃取信息的一种。由于口令的特殊性，所以将其单独列出。黑客通过登录目标主机，或使用网络监听程序进行攻击。监听到口令后，就可以顺利地登录到其他主机，或者去访问一些本来无权访问的资源。

(2) 控制中间站点

在某些情况下，黑客登上目标主机后，不是为了窃取信息，只是运行一些程序，这些程序可能是无害的，仅仅消耗一些系统的处理时间。比如，黑客为了攻击一台主机，需要一个中间站点，以免暴露自己的真实所在。这样即便被发现，也只能找到中间站点的地址，而真正的攻击者可以隐藏起来。再比如，黑客不能直接访问某一严格受控制的站点或网

络,此时就需要一个具有访问权限的中间站点,所以这个中间站点就成了首先要攻击的目标。

(3) 获得超级用户权限

黑客在攻击某一个系统时,都企图得到超级用户权限,这样就可以完全隐藏自己的行踪,并可在系统中埋伏下方便的后门,便于修改资源配置,做任何只有超级用户才能做的事情。

2. 黑客攻击的3个阶段

(1) 确定目标

黑客进行攻击,首先要确定攻击目标。比如,某个具有特殊意义的站点、某个恶意的ISP、具有敌对观点的宣传站点或解雇了黑客的单位的主页等。

(2) 搜集与攻击目标相关的信息,并找出系统的安全漏洞

信息收集的目的是为了进入所要攻击的目标网络的数据库。黑客会利用下列公开的协议或工具,收集驻留在网络系统中的各个主机系统的相关信息。

① SNMP协议,用于查阅网络系统路由器的路由表,从而了解目标主机所在网络的拓扑结构及其内部细节。

② Trace Route程序,用于获得到达目标主机所要经过的网络数和路由器数。

③ Whois协议,利用该协议的服务信息可获得所有有关DNS域和相关的管理参数。

④ DNS服务器,提供了系统中可以访问的主机的IP地址表和它们所对应的主机名。

⑤ Finger协议,用于获取一个指定主机上的所有用户的详细信息(如用户注册名、注册时间及他们是否读邮件等)。

⑥ Ping实用程序,用于确定一个指定的主机的位置。

⑦ 自编程序,如果某些产品或者系统,已经发现了一些安全漏洞,该产品或系统的厂商或组织会提供一些“补丁”程序来弥补,但是若用户没有及时打上“补丁”,黑客会利用这些漏洞来自己编写程序进入目标系统。

⑧ 利用公开的工具,如ISS(Internet security scanner)、SATAN(security analysis tool auditing network)等,这样的工具可以对整个网络或子网进行扫描,寻找安全漏洞。这样的工具既可被网络安全管理员用来作为检测网络安全性的有力武器,也可以被黑客用来作为扫描网络漏洞的黑客工具。

(3) 实施攻击

黑客在搜集到相关信息之后,就可能对目标系统实施攻击。黑客一旦获得了对攻击目标系统的访问权后,可有以下多种选择。

① 可能试图毁掉攻击入侵的痕迹,并在系统中建立另外的新的安全漏洞和后门,以使先前的攻击点被发现后,继续访问系统。

② 可能在目标系统中安装探测器软件,包括特洛伊木马程序,用来窥探所在系统的活动,收集黑客感兴趣的一切信息。

③ 可能进一步发现受损系统在网络中的信任等级,然后进一步通过该中间系统展开对整个系统的攻击。

④ 若黑客在受损系统上获得了特许访问权，就可以读取邮件、搜索和盗窃私人文件及毁坏重要数据，从而破坏整个系统的信息，造成不堪设想的后果。

⑤ 黑客在攻击得手后，往往会继续在系统中寻找相关主机的可用信息，从而攻击其他系统。

8.3　常见的网络攻击技术

8.3.1　常见的网络攻击技术

黑客的攻击手段多种多样，对常见攻击方法的了解将有助于用户达到有效防止黑客入侵的目的。

1. Web 欺骗技术

欺骗是一种主动攻击技术，它能破坏两台计算机间通信链路上的正常数据流，并可能向通信链路上插入数据。一般 Web 欺骗使用两种技术，即 URL 地址重写技术和相关信息掩盖技术。首先黑客建立一个使人相信的 Web 站点的拷贝，它具有所有的页面和链接，然后利用 URL 地址重写技术，将自己的 Web 地址加在所有真实 URL 地址的前面。这样，当用户与站点进行数据通信时，就会毫无防备地进入黑客的服务器，用户的所有信息便处于黑客的监视之中了，但由于浏览器一般均有地址栏和状态栏，用户可以在地址栏和状态栏中获得连接中的 Web 站点地址及其相关的传输信息，并由此可以发现问题，所以黑客往往在 URL 地址重写的同时，还会利用相关信息掩盖技术，以达到掩盖欺骗的目的。

2. 放置特洛伊木马程序

特洛伊木马的攻击手段就是将一些“后门”、“特殊通道”隐藏在某个软件里，将使用该软件的计算机系统成为被攻击和控制的对象。特洛伊木马程序可以直接侵入用户的计算机并进行破坏，它常被伪装成工具程序或者游戏等，诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载。一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会留在用户的计算机中，并在系统中隐藏一个可以在 Windows 启动时隐秘执行的程序。当用户连接到 Internet 时，这个程序就会通知黑客，报告用户的 IP 地址以及预先设定的端口。黑客在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改用户的计算机的参数设定、复制文件、窥视用户整个硬盘中的内容等，从而达到控制用户的计算机的目的。

3. 口令攻击

口令攻击是指先得到目标主机上某个合法用户的账号后，再对合法用户口令进行破译，然后使用合法用户的账号和破译的口令登录到目标主机，对目标主机实施攻击活动。

口令攻击方法获得用户账号的方法很多，主要是对口令的破译，常用的方法有以下

几种。

（1）暴力破解。暴力破解基本上是一种被动攻击的方式。黑客在知道用户的账号后，利用一些专门的软件强行破解用户口令，这种方法不受网段限制，但需要有足够的耐心和时间，这些工具软件可以自动地从黑客字典中取出一个单词，作为用户的口令输入给远端的主机，申请进入系统。若口令错误，就按序取出下一个单词，进行下一个尝试，直到找到正确的口令或黑客字典的单词试完为止。由于这种破译过程是由计算机程序自动完成的，因而几个小时内就可以把几十万条记录的字典里所有单词都尝试一遍。图 8.1 为"多功能密码破解软件"主界面。

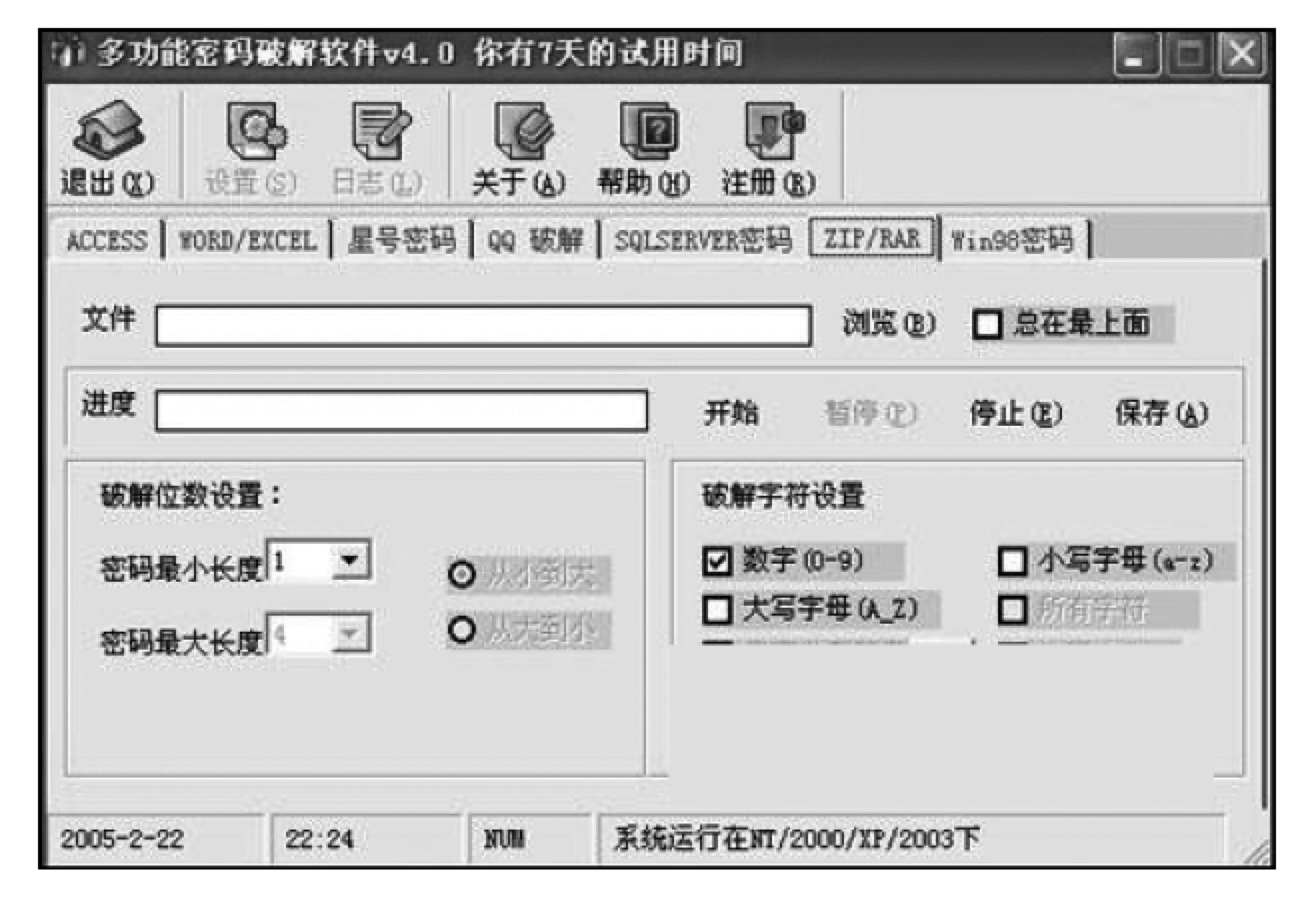


图 8.1 "多功能密码破解软件"主界面

（2）密码探测。大多数情况下，操作系统保存和传送的密码都要经过一个加密处理的过程，完全看不出原始密码的模样，而且理论上要逆向还原密码的几率几乎为零。但黑客可以利用密码探测的工具，反复模拟编码过程，并将编出的密码与加密后的密码相比较，如果两者相同，就表示得到了正确的密码。

（3）网络监听。黑客可以通过网络监听得到用户口令，这类方法有一定的局限性，但危害性极大。由于很多网络协议根本就没有采用任何加密或身份认证技术，如在 Telnet、FTP、FTTP、SMTP 等传输协议中，用户账号和密码信息都是以明文形式传输的，此时若黑客利用数据包截取工具便可很容易收集到用户的账号和密码。另外，黑客有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码。图 8.2 为 Uhack 网络监听工具，可监听经过网卡的数据包，并有简单的过滤功能。

（4）登录界面攻击法。黑客可以在被攻击的主机上，利用程序伪造一个登录界面，以骗取用户的账号和密码。当用户在这个伪造的界面上输入登录信息后，程序可记录用户的信息并传送到黑客的主机，然后关闭界面，给出提示信息"系统故障"或"输入错误"，要求用户重新输入。此时，假的登录程序自动结束，才会出现真正的登录界面。

例如，"3Q 大盗"盗号木马一般通过网页挂马或下载器下载等途径进入计算机系统。如果用户不慎感染并运行该木马，会显示出同 QQ 2010 非常相似的登录页面，而且仿真度极高，界面中还包含代理设置、软键盘、QQ 2010 登录窗口、QQ 经典登录窗口等，如图 8.3 所示。

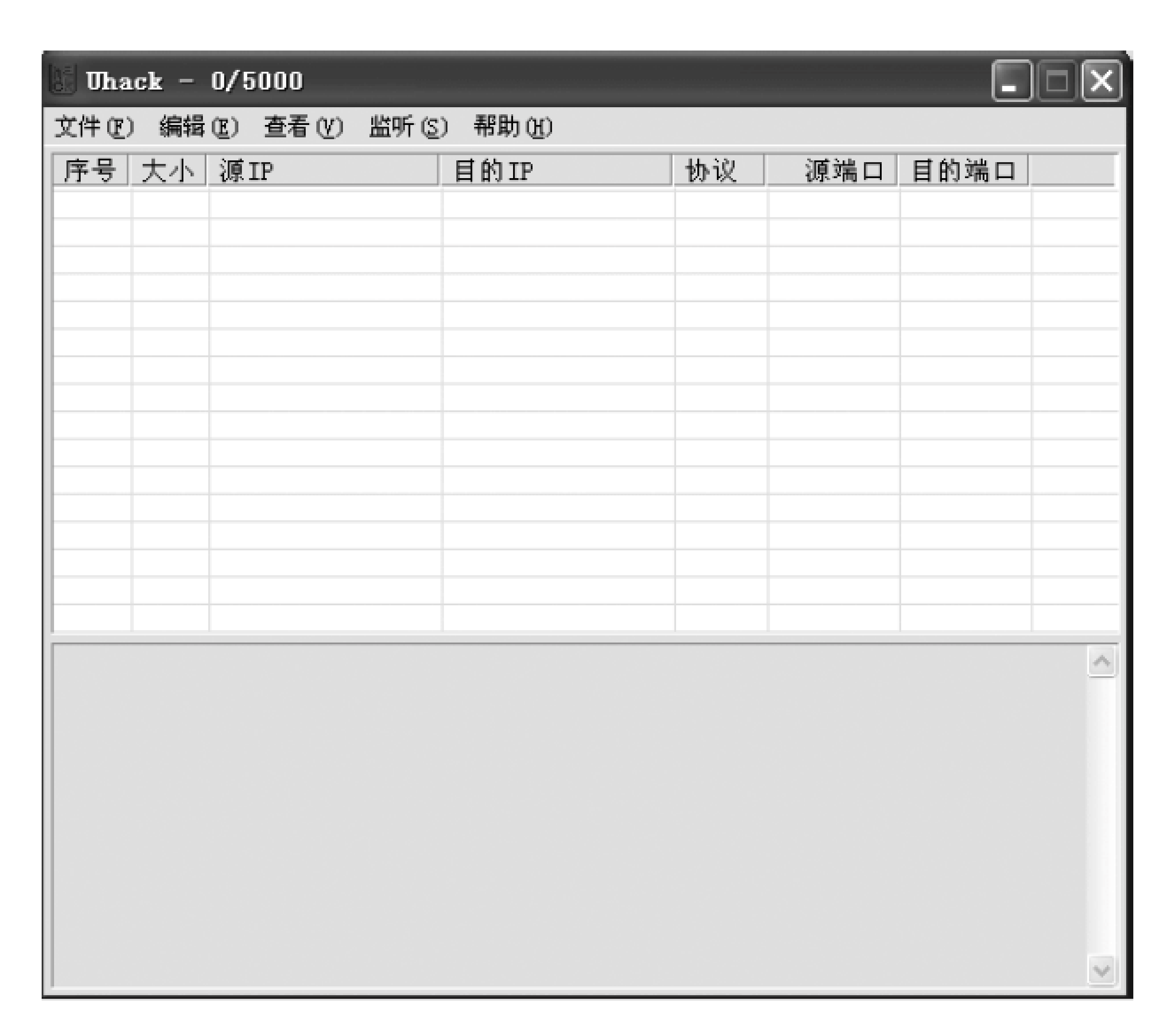


图 8.2　Uhack 网络监听工具



图 8.3　“3Q 大盗”木马模仿的 QQ 软件登录界面

4. 电子邮件攻击

电子邮件是 Internet 上运用得十分广泛的一种通信方式，但同时它也面临着巨大的安全风险。攻击者可以使用一些邮件炸弹软件向目标邮箱发送大量内容重复、无用的垃圾邮件，从而使目标邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时，还可以造成邮件系统的瘫痪。另外，对于电子邮件的攻击还包括窃取、篡改邮件数据，伪造邮件，利用邮件传播计算机病毒等。

5. 网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。网络监听可以在网上

的任何一个位置进行，如局域网中的一台主机、网关、路由设备或交换设备上，或远程网的调制解调器之间等。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，这时，黑客就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具，就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但黑客往往能够获得其所在网段的所有用户账号及口令。

6．端口扫描攻击

所谓端口扫描，就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而得知目标主机的扫描端口是否处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等。在 TCP/IP 协议中规定，计算机可以有 256×256 个端口，通过这些端口进行数据的传输。黑客一般会发送特洛伊木马程序，当用户不小心运行后，计算机内的某一端口就会打开，黑客就可通过这一端口进入用户的计算机系统。

7．缓冲区溢出

许多系统都有这样那样的安全漏洞，其中一些安全漏洞是操作系统或应用软件本身所具有的，如缓冲区溢出攻击。缓冲区溢出是一个非常普遍、危险的漏洞，在各种操作系统、应用软件中广泛存在。产生缓冲区溢出的根本原因在于，将一个超过缓冲区长度的字串拷贝到缓冲区。溢出带来了两种后果，一是过长的字串覆盖了相邻的存储单元，引起程序运行失败，严重的可引起死机、系统重新启动等后果；二是利用这种漏洞可以执行任意指令，甚至可以取得系统特权。针对这些漏洞，黑客可以在长字符串中嵌入一段代码，并将过程的返回地址覆盖为这段代码的地址。当过程返回时，程序就转而开始执行这段黑客自编的代码了。一般来说，这段代码都是执行一个 Shell 程序。这样，当黑客入侵一个带有缓冲区溢出缺陷且具有 Suid-root 属性的程序时，就会获得一个具有 Root 权限的 Shell，在这个 Shell 中黑客可以干任何事。恶意地利用缓冲区溢出漏洞进行攻击，可以导致运行失败、系统死机、重启等后果，更为严重的是，可以利用它执行非授权指令，甚至可以取得系统特权，进而进行各种非法操作，取得计算机的控制权。

8.3.2 拒绝服务攻击

1．拒绝服务攻击简介

拒绝服务（denial of service，DoS）攻击大致可以分为两类。一类 DoS 攻击是由于错误配置或者软件弱点导致的，某些 DoS 攻击是由于协议固有的缺陷或者对协议的实现导致的，这类攻击可以通过开发商发布简单的补丁来解决；另一类 DoS 攻击利用合理的服务请求来占用过多的服务资源，致使服务超载，无法响应其他的请求。这些服务资源包括网络带宽、文件系统空间容量、CPU 时间等。这种攻击会导致系统资源的匮乏。无论计算机的处理速度多么快，内存容量多么大，网络的带宽有多少，都总有一个极限，所以，总

能找到一种方法使请求的值大于该极限值,对于这类攻击还没有一个固定的解决方案。

长期以来,第一类 DoS 攻击,也就是由于错误配置或者软件弱点导致的攻击是攻击的主流方式。这是因为利用合理的服务请求来占用过多的服务资源,这种攻击方法往往需要相当大的带宽,而高带宽是大公司和国家科研机关所拥有的,以个人为主的黑客很难享用。为了克服这个缺点,攻击者开发出分布式攻击技术,利用工具集合许多的网络带宽来对同一个目标发送大量的请求,这就引入了一个新概念:分布式。这些程序可以使得分散在 Internet 各处的机器共同完成对一台主机攻击的操作,从而使主机看起来好像是遇到了不同位置的许多主机的攻击。这些分散的机器通过由几台主控制机操作来进行多种类型的攻击,如 UDP flood、SYN flood 等。

DoS 攻击的一个特点是这种攻击通常无法追踪。由于这种攻击一般不需要与目标之间的交互,所以攻击者可以伪造 IP 地址。在 UNIX 环境中伪造源 IP 地址非常容易,不过这需要攻击者具有 root 权限。

2. 常见的拒绝服务攻击

(1) flood

flood 是“淹没”的意思,它是 DoS 攻击的一种手法,具有高带宽的计算机可以通过大量发送 TCP、UDP 或者 ICMP echo request 的报文,将低带宽的计算机“淹没”,降低对方计算机的响应速度。其中最简单的一种办法就是在 UNIX 下使用 Ping-IP,这种通过发送异常的、大的 Ping 来杀掉服务器的方法有时称为 ping of death。另一种常用的手法称为 SYN flood,攻击者有意不完成 TCP 的 3 次握手过程,其目的是让等待建立某种特定服务的连接数量而超过系统所能承受的数量,从而使系统不能建立新的连接。

虽然所有的操作系统对每个连接都设置了一个计时器,如果计时器超时就释放资源,但是攻击者可以持续建立大量新的 SYN 连接来消耗系统资源。很显然,由于攻击者并不想完成 3 次握手过程,所以不需要接收 SYN/ACK,因此,也就没有必要使用真实的 IP 地址。实现 SYN flood 是非常简单的,在 Internet 上有大量的源程序可以下载。

(2) Smurf

Smurf 是一种很古老的 DoS 攻击,这种方法使用了广播地址(broadcast address)。发向广播地址的 IP 包会被网络中所有的计算机所接收,广播地址的尾数通常为 0,如 192.168.1.0,尾数为 255 的地址通常作为多播地址(multicast address),但有时候也被用作广播地址。

设想发送一个 IP 包到广播地址 192.168.1.0,假设这个网络中有 50 台计算机,将会收到 50 次应答,广播地址在这里起到了放大器的作用,Smurf 攻击就利用了这种作用。如果 A 发送 1KB 大小的 ICMP echo request 到广播地址,那么 A 将收到 1KB×N 的 ICMP Reply,其中,N 为网络中计算机的总数。当 N 等于 100 万时,产生的应答将达到 1GB,这将会大量消耗网络资源,如果 B 假冒了 A 的 IP 地址,那么收到应答的是 A,对 A 来说就是一次拒绝服务攻击。最经典的 Smurf 程序称为 parasmurf.c。

(3) Teardrop

在早期 BSD UNIX 实现的网络协议中,在处理数据包分段时存在漏洞,后来的一些

操作系统都沿用了BSD的代码，所以这个漏洞在Linux、Windows 2000和Windows 2003中都是存在的。物理网络层通常给所能传输的帧加一个尺寸上限，IP将数据报的大小与物理层的帧的上限进行比较，如果需要则进行分段。在IP报头中设置了一些域用于分段：其中标志域为发送者传输的每个报文保留一个独立的值，这个数值被复制到每个特定报文的每个分段，标志域中有一位作为“更多分段”位，除了最后一段外该位在组成一个数据报的所有分段中被置位；分段偏移域（fragment offset）含有该分段自初始数据报开始位置的位移。对于有Teardrop漏洞的操作系统，如果接收到“病态的”数据分段，例如一个40B的数据报被分为两段，第一段数据发送0～36B，而第二段发送24～27B，在某些情况下会破坏整个IP协议栈，只有必须重新启动计算机才能恢复。

3. 拒绝服务攻击的防范方法

RFC 2267建议在全球范围的Internet路由器上使用向内过滤的机制防止假冒地址的攻击，使得外部机器无法假冒内部机器的地址来对内部机器发动攻击。但是这种办法应用起来存在太大的闲难，ISP往往并不是很关心这类安全问题。

从目前的情况来看，为了防御拒绝服务攻击，很多商业网站都采用DNS轮循，或者通过负载均衡、Cluster等技术来增加响应主机数量，但这样做的成本是很高的。

绿盟科技(www.nsfocus.com)开发的抗拒绝服务攻击产品“黑洞”是防拒绝服务攻击这个领域非常领先的产品。据绿盟介绍，“黑洞”能够对SYN flood、UDP flood、ICMP flood和stream flood等各类DoS攻击进行防护。可以防止连接耗尽，对典型“以小博大”的资源比拼型攻击（如大规模的多线程下载）也具有良好的防护能力。由于可以给各种端口扫描软件反馈迷惑性信息，因此，也可以对其他类型的攻击起到保护作用。

8.3.3 特洛伊木马攻击

特洛伊木马就是我们平常所说的木马，名称取自希腊神话特洛伊木马，它是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。这里的隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现感染了木马病毒，也很难确定其具体位置。非授权性是指控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件、修改注册表、控制鼠标和键盘等，而这些权利并不是服务端赋予的，而是通过木马程序窃取的。

从木马的发展来看，可以分为两个阶段。最初网络还处于以UNIX平台为主的时期，木马就产生了，当时木马程序的功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些木马的功能。这个时期木马的设计者和使用者大都是一些技术人员，具备了相当的网络和编程知识。后来，随着Windows平台的日益普及，一些基于图形操作的木马程序出现了，改善后的用户界面更加友好，使用者不需要懂得太多的专业知识就可以熟练地操作木马。木马的使用者增加了，相应的木马入侵事件也频繁出现，而且由于这个时期木马的功能日趋完善，因此对服务端的破坏性也更大了。

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。硬件部分是指建立木马连接所必需的硬件实体。前面曾经提到控制端和服务端，控制端指的是对服务端

进行远程控制的一方。服务端是指被控制端远程控制的一方。而 Internet 则是控制端对服务端进行远程控制、传输数据的网络载体。软件部分是实现远程控制所必需的软件程序,包括控制端程序、木马程序及木马配置程序。其中,控制端程序是控制端用以远程控制服务端的程序;木马程序是指潜入服务端内部,获取其操作权限的程序;木马配置程序是指设置木马程序的端口号、触发条件和木马名称等,这个程序主要是为了让木马在服务端更隐藏。具体连接部分是指木马进行数据传输的目的地。

根据木马程序的用途,木马程序可以分为网络游戏木马、网银木马、即时通信软件木马、网页点击类木马、下载类木马、代理类木马。

1. 配置木马

对木马进行配置的主要目的是实现木马的伪装和信息反馈两个功能。木马的伪装是指为了更好地隐藏木马,采用多种伪装手段,如修改图标、捆绑文件或定制端口等诸多方式。信息反馈是指木马配置程序将信息反馈的方式或地址进行设置,如设置信息反馈的邮件地址或 QQ 号等。

具体而言,木马的伪装形式包括以下几种。

(1) 修改图标。用户在接收到的邮件的附件中看到文本文件的图标时,里面可能隐藏着木马程序。因为现在已经有可以将木马服务端程序的图标改成 HIML、TXT 或 ZIP 等文件图标的专门技术。当然,目前提供这种功能的木马还不是很多,并且这种伪装也不是无懈可击的。

(2) 捆绑文件。这种伪装手段是将木马捆绑在一个安装程序上,当安装程序运行时,木马在用户毫无察觉的情况下进入了系统。

(3) 出错提示。有一定木马知识的人都知道,如果欲打开一个文件却没有任何反应,这很可能就是个木马程序。木马的设计者为了弥补这个缺陷,就为木马提供了一个出错显示的功能。当服务端用户打开木马程序时,会弹出一个伪造的错误提示框,内容可以自定义,如“文件无法打开!”。

(4) 定制端口。老式的木马程序所使用的端口一般都是固定的,利于判断是否感染木马。木马的设计者为了弥补这个缺陷,为木马提供了一个叫作定制端口的功能。控制端用户可以选择任意一个大于 1024 的端口作为木马端口,为判断木马带来了困难。

(5) 自我销毁。当服务端打开含有木马的文件后,木马会将自己拷贝到操作系统的系统文件中。一般来说,原木马文件的大小和系统文件夹中的大小是一样的,感染了木马的用户只要在收到的邮件和下载的软件中找到原木马文件,在系统文件夹中找到相同大小的文件,就可以判断木马确实存在了。而木马的自我销毁功能是指安装完木马后,原木马文件将自动销毁,这样服务端用户就很难找到木马的来源。

(6) 木马更名。安装到系统文件夹中的木马的文件名一般是固定的,那么只要根据一定的常规知识,找到特定的文件,就可以知道中了什么木马。而现在有很多木马都允许控制端用户自由定制安装后的木马文件名,这样就很难判断所感染的木马类型了。

2. 传播木马

传播木马的方式主要有两种：一种是通过电子邮件，控制端将木马程序以附件的形式随同邮件发送；而另一种是软件下载，一些非正规的网站以提供软件下载的名义，将木马捆绑在软件安装程序上，程序下载后，只要一运行，木马就会自动安装。

3. 运行木马

木马自动安装后，首先将自己拷贝到操作系统的系统文件夹中，然后在注册表、启动组及非启动组中设置好木马的触发条件，这样木马的安装就完成了。安装后就可以启动木马了。木马的运行过程如下：设置木马的触发条件，木马进入内存，然后开启相应的端口。运行后的木马会将服务端的相关信息泄露给控制端，并在开放的端口等候控制端的连接。

触发条件是指启动木马的条件，大致出现在以下几个地方。

(1) 注册表[HKEY-LOCAL-MACHINE\Software\Microsoft\Windows\CurrentVersion\]的 Run 和 RunSerices 主键。

(2) system.ini 文件中在[386enh]、[mci]和[drivers32]内有关于启动木马的命令行。

(3) 文件 autoexec.bat 和 config.sys 及应用程序的启动配置文件也可以启动木马。这种加载方式一般都需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传服务端覆盖这两个文件才行。

(4) 注册表[HKEY-CLASSES-ROOT\文件类型\shell\open\command]主键。例如，国产木马“冰河”就是通过修改此键，将“C:\Windows\SYSTEM\sysexplr.exe%1”改为“C:\Windows\system\sysexplr.exe%1”。双击一个文本文件后，原本应打开记事本的程序都变成启动木马程序了。通过修改.html、.exe 及.zit 等文件的启动命令的键值都可以启动木马。

(5) 捆绑文件。实现这种触发条件要控制端和服务端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，上传到服务端覆盖文件。这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马又会被运行安装。

(6) “启动”菜单。在“开始”→“程序”→“启动”选项下也可能有木马的触发条件。

木马运行时都在开放端口，如果在脱机状态下查看到有端口开放，或上网时，有一些数值比较大的端口开放，那就要小心查看是否已经感染木马了。

4. 信息泄露

设计成熟的木马都有信息反馈机制，这里的信息反馈是指木马成功安装后会收集一些服务端的软、硬件信息，并通过相关的方式反馈给控制端用户。泄露的信息包括操作系统、系统目录、硬盘分区情况和系统口令等。在这些信息中，最重要的是服务端的 IP 地址。

5. 建立连接

有了IP地址之后，木马连接就可以建立起来，这样，控制端端口和木马端口之间就会出现一条通道。而控制端上的控制端程序就可以通过这条通道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制。

6. 远程控制

控制端能享有的控制权限有以下几种。

（1）窃取密码。一切以明文形式或缓存在Cache中的密码都能被木马侦测到，此外很多木马还提供击键记录功能，它将会记录服务端每次敲击键盘的动作。一旦木马入侵，用户密码将很容易被窃取。

（2）文件操作。控制端可由远程控制对服务端上的文件进行删除、新建、修改、上传、下载、运行和更改属性等一系列操作。

（3）修改注册表。控制端可任意修改服务端注册表，包括删除、新建或修改主键、子键或键值。这样，控制端就可以禁止服务端软驱和光驱的使用，锁住服务端的注册表，将服务端上木马的触发条件设置得更隐蔽，从而完成一系列高级操作。

（4）系统操作。这项内容包括重启或关闭服务端操作系统、断开服务端的网络连接、控制服务端的鼠标和键盘、监视服务端桌面操作、查看服务端进程及控制端，甚至可以随时给服务端发送信息。

随着网络的普及，上网的人或多或少都要受到木马的困扰。木马主要是通过下载软件和电子邮件两种途径传播。所以，为了避免感染木马用户首先要到正规的网站去下载软件。然后，在接收邮件的时候，一定要谨慎地观察附件。如果附件是.exe文件或者是一些不常见的文件类型，有可能是木马。另外，前面曾经提及木马也可以将图标伪装成.txt或.html，这样就要看附件的长度了，一个木马程序一般都要100KB以上，而.txt或.html就不会这么大了。最后，就是看打开附件之后的反应了，如果打开附件毫无反应，或者是弹出一个出错提示框，那可能就是木马了。



【案例】“灰鸽子”的攻击

案例分析

“灰鸽子”是国内一款著名后门程序，比起“冰河”、“黑洞”来，“灰鸽子”可以说是国内后门的集大成者。其丰富而强大的功能、灵活多变的操作、良好的隐藏性等，使其他后门工具都相形见绌。而其客户端简易便捷的操作，使刚入门的初学者也可充当黑客。

操作环境

Windows Server 2003、Windows XP系统。

操作步骤

第1步　将“灰鸽子”软件下载并安装之后，即可通过“开始”菜单或桌面上的“灰鸽

子”快捷方式进入客户端操作窗口，如图 8.4 所示。在运用“灰鸽子”软件之前，需要先在自己的本地机上生成木马的服务端。



图 8.4 黑防版“灰鸽子”主界面

第 2 步 选择“文件”→“配置服务程序”命令，即可打开“服务器配置”窗口，如图 8.5 所示。



图 8.5 “服务器配置”窗口

第 3 步 在“安装选项”选项卡中可以设置将服务器程序安装到哪个目录、安装名称等信息，并选择“安装成功后自动删除安装文件”选项，如图 8.6 所示。

第 4 步 选择“启动项设置”选项卡，然后在几个文本框中输入相关信息，如图 8.7 所示。

第 5 步 选中“高级选项”选项卡，如图 8.8 所示。



图 8.6　“安装选项”选项卡

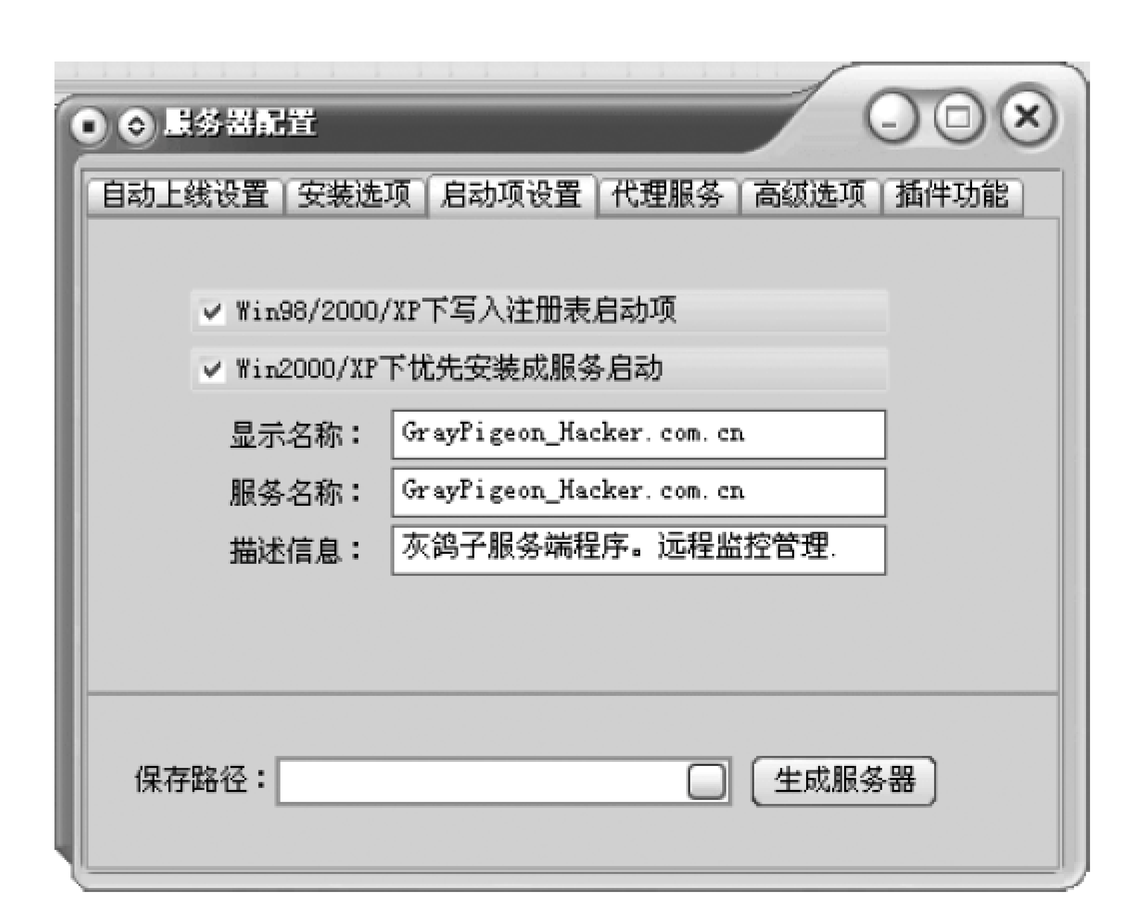


图 8.7　“启动项设置”选项卡



图 8.8　“高级选项”选项卡

第 6 步 在“保存路径”文本框中输入生成的服务端程序的保存路径及文件名。最后单击“生成服务器”按钮，即可生成服务端程序，如图 8.9 所示。

将“灰鸽子”服务端程序发送给目标并成功安装之后，使用客户端就可以远程控制目标计算机了。

第 7 步 为了使客户端收到服务端自动上线的信息，还需要对客户端的自动上线进行设置，选择客户端主窗口中的“文件”→“自动上线”命令进入图 8.10 中进行设置，设置完成后，单击“更新 IP 到 FTP 空间”按钮，如图 8.11 所示，则 FTP 更新 IP 文件成功。



图 8.9 配置服务器程序成功



图 8.10 自动上线设置

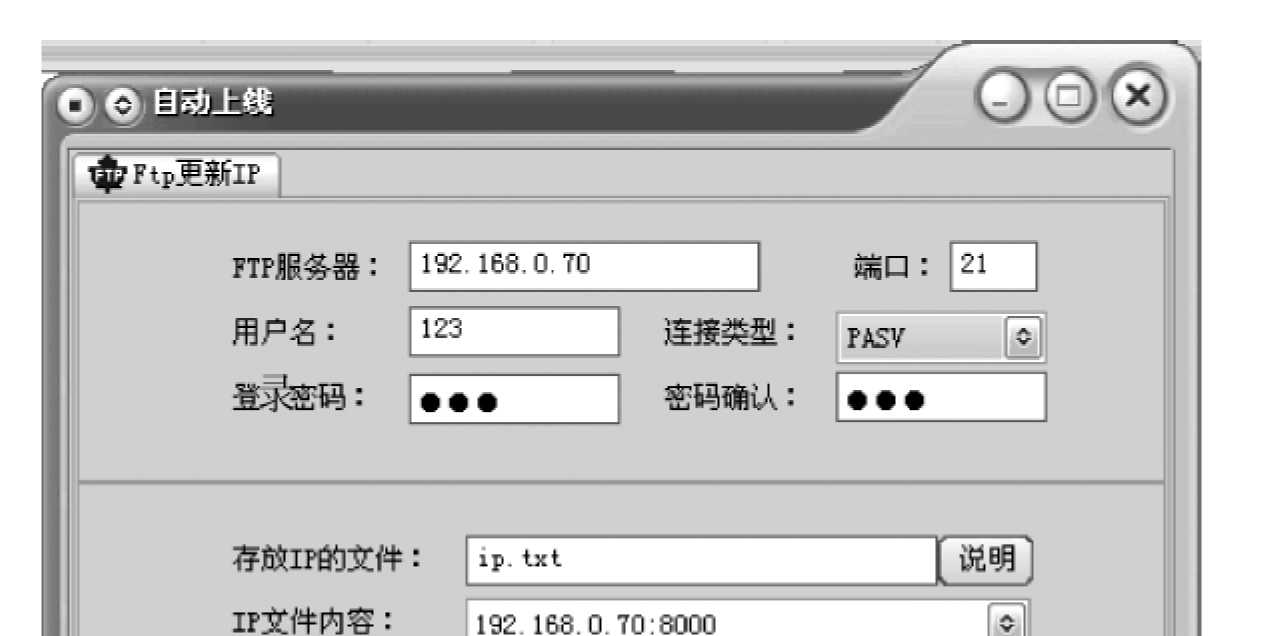


图 8.11 更新成功

第 8 步 展开文件目录浏览中的自动上线主机，主机上线，如图 8.12 所示。

第 9 步 文件控制。当客户端与服务端正常连接之后，用户就可以远程控制服务端计算机了。

在“灰鸽子”客户端界面中，打开“文件管理器”选项卡，单击需要远程控制的计算机名称前的折叠按钮，即可查看该远程计算机上的文件，并可以实现文件的上传与下载，如图 8.13 所示。



图 8.12　主机上线



图 8.13　“文件管理器”选项卡

第 10 步　远程控制命令。打开“远程控制命令”选项卡，即可实现对远程计算机进行重启、关闭、查看远程计算机系统信息、查看和结束远程计算机进程、查看和控制远程计算机服务、查看远程或本地剪贴板内容、查看远程计算机共享信息等操作，如图 8.14 所示。

第 11 步　注册表编辑器。打开“注册表编辑器”选项卡，即可查看和编辑远程计算机注册表，如图 8.15 所示。



图 8.14 “远程控制命令”选项卡



图 8.15 “注册表编辑器”选项卡

第 12 步 命令广播。打开“命令广播”选项卡，在“常用命令广播”子选项卡中，用户可以卸载远程计算机中的“灰鸽子”服务端程序、重启或关闭远程计算机，以及通过远程计算机打开网页和从远程计算机下载文件，如图 8.16 所示。

此外，在“命令广播”选项卡中用户还可以向远程计算机发送消息、筛选符合条件的主



图 8.16 "命令广播"选项卡

机、批量修改备注。

第 13 步 屏幕控制。单击工具栏上的"捕获屏幕"按钮，即可打开"捕获屏幕"窗口，如图 8.17 所示。



图 8.17 屏幕控制

单击工具栏上的"传送鼠标和键盘操作"按钮，客户端即可远程控制目标计算机的屏幕操作。单击"发送组合键"按钮，即可远程控制目标计算机的屏幕操作。单击"发

送组合键”按钮，即可从弹出的菜单中选择系统发送的组合键命令。

单击“保存”按钮，即可将当前远程计算机屏幕保存下来，还可以将远程计算机屏幕操作记录为 MPEG 文件，以供浏览。

第 14 步 视频语言。通过视频语言功能，用户可以与远程计算机进行语言交流，并可将远程计算机摄像头数据记录成 MPEG 文件。此外，“灰鸽子”远程控制程序还具有一般远程控制都具有的 Telnet 功能，如图 8.18 所示。



图 8.18 Telnet 功能

8.4 常见的攻击工具

8.4.1 邮件炸弹工具

所谓的电子邮件炸弹，指的是邮件发送者利用特殊的电子邮件软件，在很短的时间内连续不断地将邮件邮寄给同一个收信人，在这些数以千万计的大容量信件面前收件箱肯定不堪重负，而最终“爆炸身亡”。目前，知名的邮件炸弹有 E-mail Bomb、KaBoom3、Unabomb 等。

这种攻击手段不仅会干扰用户的电子邮件系统的正常使用，甚至还能影响到邮件系统所在的服务器系统的安全，造成整个网络系统全部瘫痪，所以邮件炸弹具有很大危害。

邮件炸弹可以大量消耗网络资源，常常导致网络塞车，使大量的用户不能正常地工作。通常，网络用户的信箱容量是很有限的，在有限的空间中，如果用户在短时间内收到成千上万封电子邮件，那么经过一轮邮件炸弹轰炸后的电子邮件的总容量很容易就把用户有限的阵地挤垮。这样用户的邮箱中将没有多余的空间接纳新的邮件，那么新邮件将会被丢失或者被退回，这时用户的邮箱已经失去了作用；另外，这些邮件炸弹所携带的大容量信息不断在网络上来回传输，很容易堵塞带宽并不富裕的传输信道，加重服务器的工作强度，导致服务器处理电子邮件整个过程的延迟。

预防炸弹袭击的措施如下。

(1) 向 ISP 求援。一旦信箱被轰炸了，但自己又没有好的办法来对付它，这时应该向 ISP 服务商求援，它们会采取办法清除 E-mail Bomb。

(2) 采用过滤功能。在邮件软件中安装一个过滤器(如 E-mail Notify)是一种最有效的防范措施。在接收任何电子邮件之前预先检查发件人的资料，如果觉得有可疑之处，可以将之删除，不让它进入用户的邮件系统。但这种做法有时会误删除一些有用的邮件。如果担心有人恶意破坏你的信箱，给你发来一个“重磅炸弹”，可以在邮件软件中启用过滤功能，把邮件服务器设置为超过信箱容量的大邮件时自动删除。

(3) 使用转信功能。有些邮件服务器为了提高服务质量往往设有“自动转信”功能，利用该功能可以在一定程度上解决容量特大邮件的攻击问题。假设用户申请了一个转信信箱，利用该信箱的转信功能和过滤功能，可以将那些不愿意看到的邮件统统过滤掉，删除在邮件服务器中，或者将垃圾邮件转移到自己其他免费的信箱中，或者干脆放弃使用被轰炸的邮箱，另外重新申请一个新的信箱。

(4) 谨慎使用自动回信功能。所谓“自动回信”就是指对方给用户的这个信箱发来一封信而用户如果没有及时收取，邮件系统会按照用户事先的设定自动给发信人回复一封确认收到的信件。这个功能本来给大家带来了方便，但也有可能制造成邮件炸弹！试想一下，如果给用户发信的人使用的邮件账号系统也开启了自动回信功能，那么当用户收到他发来的信而没有及时收取时，用户的系统就会给他自动发送一封确认信。恰巧他在这段时间也没有及时收取信件，那么他的系统又会自动给用户发送一封确认收到的信。如此一来，这种自动发送的确认信便会在双方的系统中不断重复发送，直到把用户双方的信箱都撑爆为止。

(5) 用专用工具来对付。如果用户的邮箱不幸已经“中弹”，而且用户还想继续使用这个信箱名的话，可以用一些邮件工具软件如 PoP-It 来清除这些垃圾信息。这些清除软件可以登录到邮件服务器上，使用其中的命令来删除不需要的邮件，保留有用的信件。

8.4.2 扫描工具

扫描工具是一种能够自动检测远程或本地主机安全弱点的程序，通过它可以获得远程计算机的各种端口分配及提供的服务和它们的版本。扫描器攻击时是通过选用不同的 TCP/IP 端口的服务，并记录目标主机给予的应答，以此搜集到关于目标主机的各种有用信息，而不是直接进攻，它获取的信息必须经过人为的分析才能成为真正有用的信息。当然，这需要用户具有一定的网络知识，否则，扫描器对于用户来说，将毫无用处。

下面介绍两种有名的扫描器。

1. 流光

流光是集端口扫描、字典工具、入侵工具、口令猜解于一身的多功能扫描器。它能让一个刚刚会用鼠标的人成为专业级黑客。它可以探测 POP3、FTP、SMTP、IMAP、SQL、IPC、IIS、FINGER 等各种漏洞，并针对各种漏洞设计了不同的破解方案，能够在有漏洞的系统上轻易得到被探测的用户密码。流光对 Windows 2000/XP 上的漏洞都可以探测，使它成为黑客手中必备的工具之一。

流光的功能非常强大,它支持163/169双通和多线程检测,支持高效的用户流模式和高效服务器流模式,可同时对多台POP3/FTP主机进行检测,它支持最多500个线程控测,当线程超时设置时,阻塞线程具有自杀功能,不会影响其他线程。流光还支持10个字典同时检测。并且检测设置可作为项目保存。

2. SuperScan

SuperScan是一个功能强大的端口扫描工具。它可以通过Ping来检验目标计算机是否在线,支持IP和域名相互转换,还可以检验一定范围内目标计算机的端口情况和提供的服务类别。SuperScan可以自定义要检验的端口,并可以保存为端口列表文件,它还自带了一个端口列表,通过这个列表可以检测目标计算机是否有木马,同时用户也可以自己定义、修改以上木马端口列表。在SuperScan找到的主机上,右击可以实现HTTP浏览、Telnet登录、FTP上传、域名查询等功能,界面如图8.19所示。



图8.19 SuperScan 4.0界面

SuperScan扫描时的速度非常快,而且CPU占用率也非常小、非常平稳,甚至感觉不到它的运行。同时,SuperScan扫描时占用的带宽也非常小,在使用宽带和电话拨号网络时,几乎没有什么差别。SuperScan很适合扫描整个网段中的特定端口,用它做端口范围1～65535的扫描也非常适合,所以,许多人把SuperScan作为扫描肉鸡及制作SOCK代理的必备工具。其缺点是扫描时,有些端口无法扫描到。



【案例】 端口扫描工具SuperScan的使用

案例分析

SuperScan是一个功能强大的端口扫描工具。它可以通过Ping来检验目标计算机是否在线,支持IP和域名相互转换,还可以检验一定范围内目标计算机的端口情况和提

供的服务类别。

操作环境

Windows Server 2003、Windows XP 系统。

操作步骤

第 1 步 扫描 IP 地址。

下载并给 SuperScan 4.0 解压后，双击 SuperScan.exe，开始使用。打开主界面，默认为扫描(Scan)菜单，允许用户输入一个或多个主机名或 IP 范围。也可以选文件下的输入地址列表。输入主机名或 IP 范围后开始扫描，单击▶按钮，SuperScan 开始扫描地址，如图 8.20 所示。

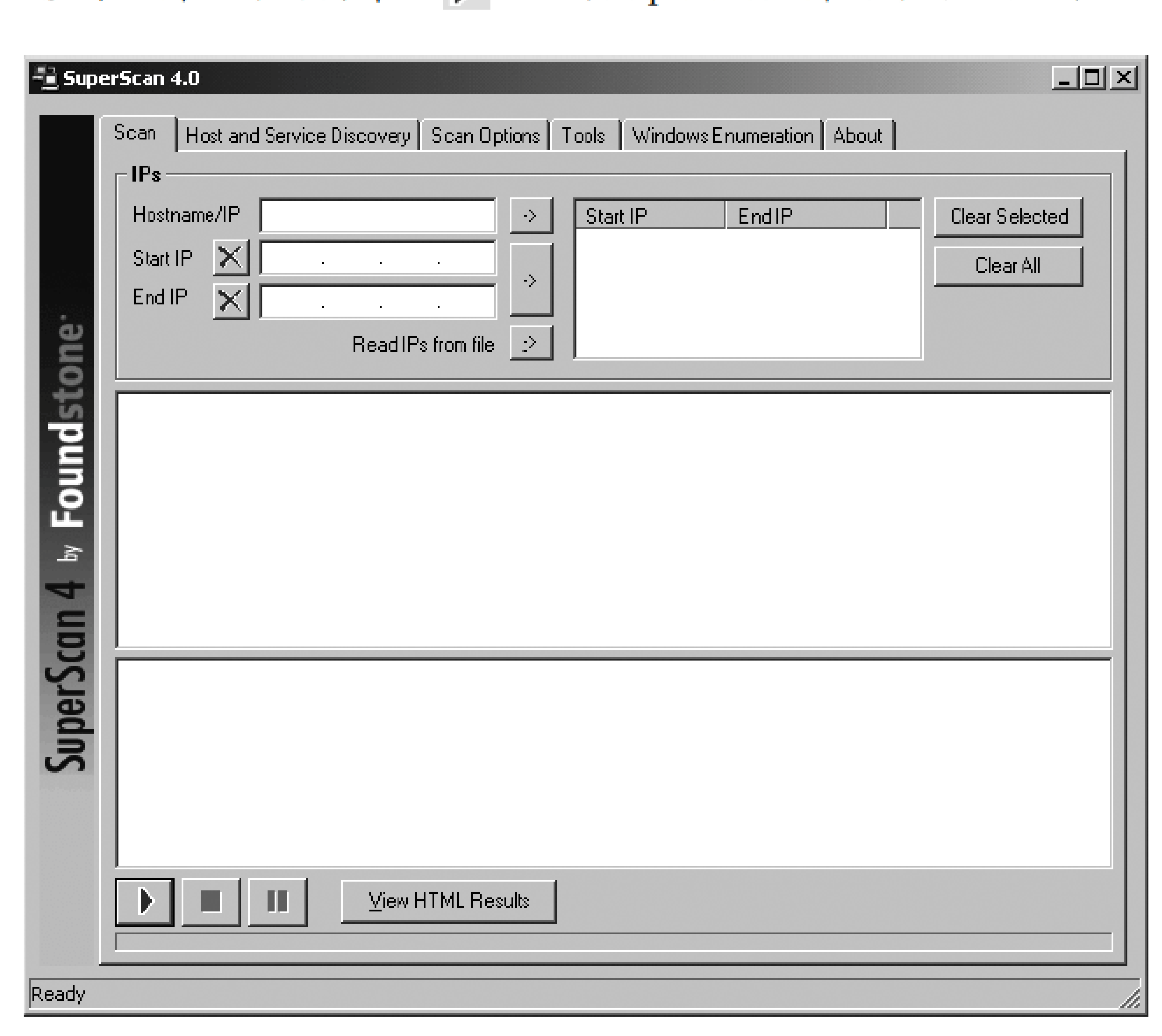


图 8.20 SuperScan 在指定的 IP 范围内扫描

扫描进程结束后，SuperScan 将提供一个主机列表，关于每台扫描过的主机被发现的开放端口信息。SuperScan 还有选择以 HTML 格式显示信息的功能，如图 8.21 所示。

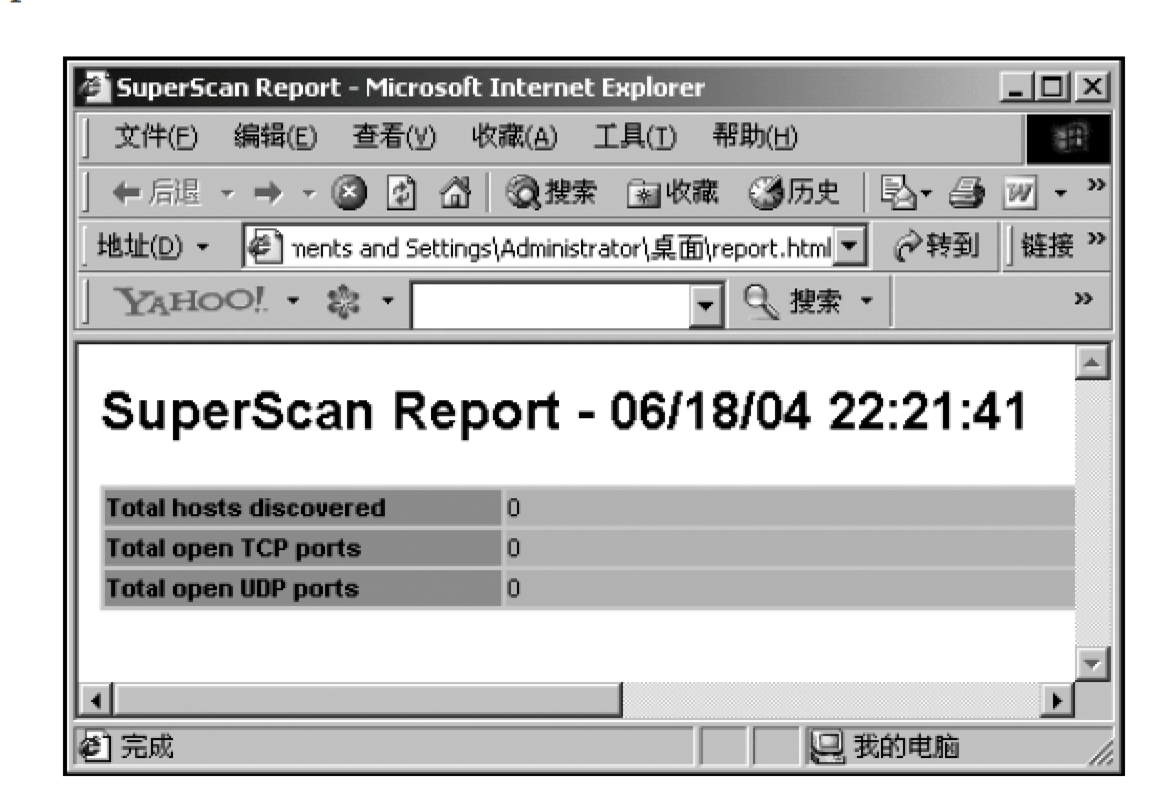


图 8.21 SuperScan 显示扫描的主机和在每台主机上开放的端口

第 2 步　进行主机和服务器扫描设置。

(1) 这是从一群主机中执行简单的扫描,然而很多时候需要定制扫描。图 8.22 上看到的是 Host and Service Discovery 选项。这个选项在扫描的时候可看到更多信息。

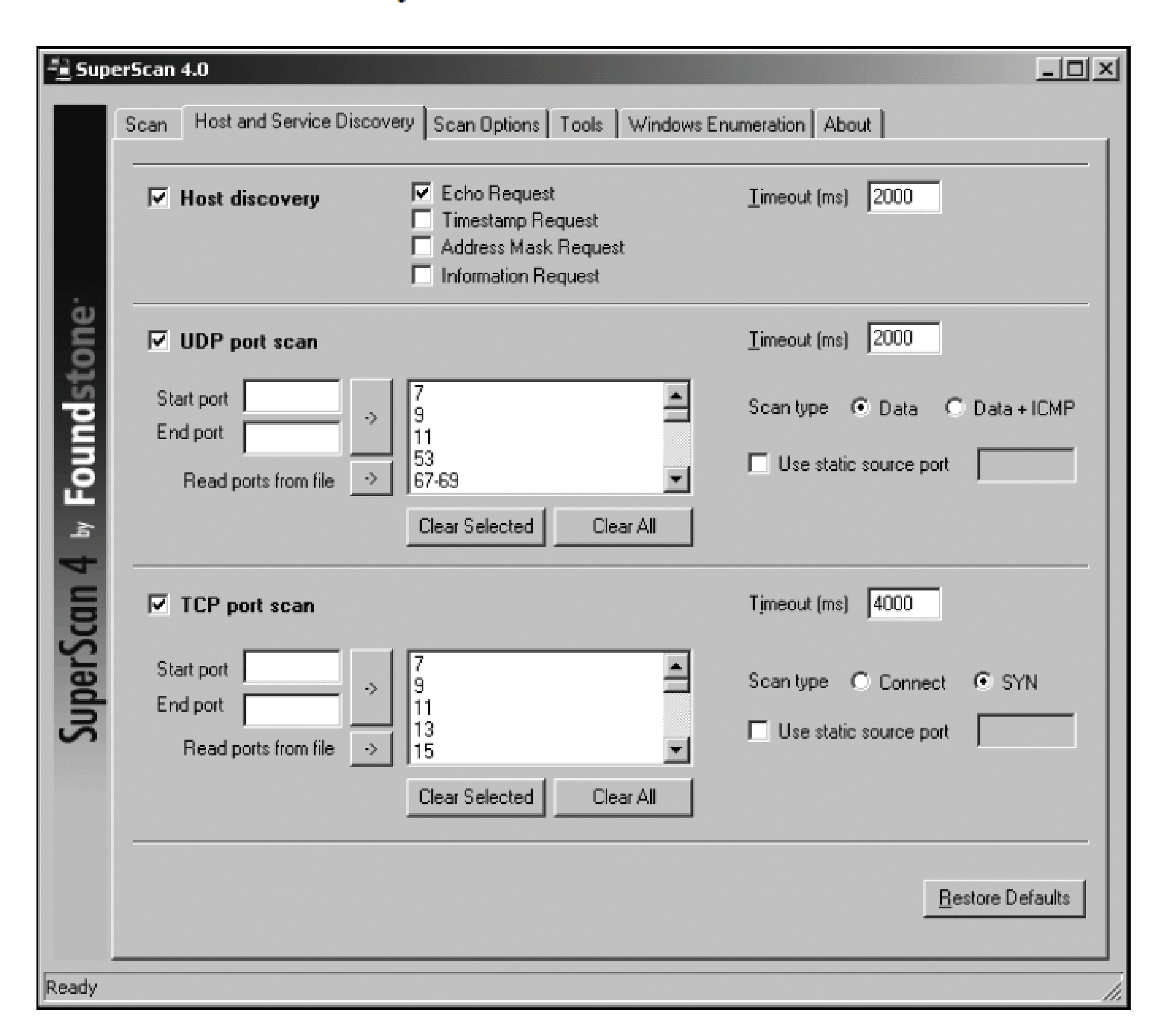


图 8.22　Host and Service Discovery 扫描界面

(2) 在菜单顶部是 Host discovery 复选框,发现主机的默认方法是通过重复请求(Echo Requests)。通过选择和取消各种可选的扫描方式选项,也能够通过利用时间戳请求(Timestamp Request)、地址屏蔽请求(Address Mask Requests)和消息请求(Information Requests)来发现主机。应该注意的是,用户选择的选项越多,那么扫描用的时间就越长。如果用户试图尽量多地收集一个明确的主机的信息,建议首先执行一次常规的扫描以发现主机,然后再利用可选的请求选项来扫描。在菜单的底部,包括 UDP 端口扫描和 TCP 端口扫描项。通过屏幕的截图,注意到 SuperScan 最初开始扫描的仅仅是那几个最普通的常用端口。原因是有超过 65 000 个的 TCP 和 UDP 端口。若对每个可能开放端口的 IP 地址,进行超过 130 000 次的端口扫描,那将需要更长的时间。因此,SuperScan 最初开始扫描的仅仅是那几个最普通的常用端口,但给用户扫描额外端口的选项。

第 3 步　使用扫描选项。

如图 8.23 所示,Scan Options 选项卡允许进一步地控制扫描进程。菜单中的首选项是定制扫描过程中主机和通过审查的服务数。1 是默认值,一般来说已足够,除非不太可靠。

Scan Options 中接下来的选项,能够设置主机名解析的数量。同样,数量 1 足够了,除非用户的连接不可靠。另一个选项是获取标志(Banner Grabbing)的设置,Banner Grabbing 是根据显示一些信息尝试得到远程主机的回应。默认的延迟是 8000 毫秒,如果用户所连接的主机较慢,这个时间就显得不够长。

窗口右侧旁边的滑块是扫描速度调节选项,能够利用它来调节 SuperScan 在发送每

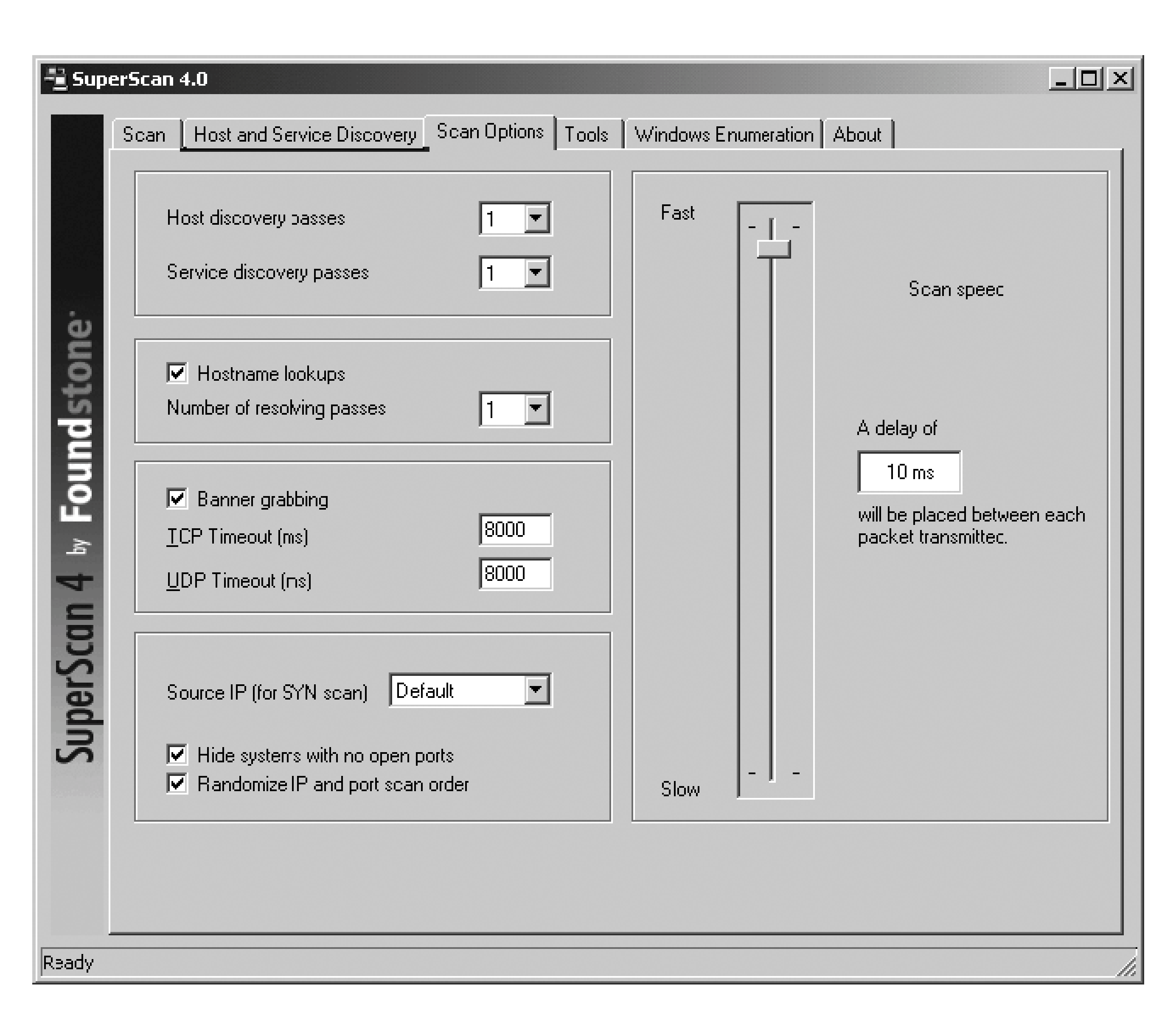


图 8.23　Scan Options 选项界面

个包所要等待的时间。最快的可能扫描，当然是调节滚动条为 0。可是，扫描速度设置为 0，有包溢出的潜在可能。如果用户担心由于 SuperScan 引起的过量包溢出，最好调慢 SuperScan 的速度。

第 4 步　使用工具选项。

使用 SuperScan 的工具选项允许用户很快得到许多关于一个明确的主机信息。正确输入主机名或者 IP 地址和默认的连接服务器，然后单击要得到相关信息的按钮。如用户 Ping 一台服务器或 traceroute 和发送一个 HTTP 请求。图 8.24 显示了得到的各种信息。

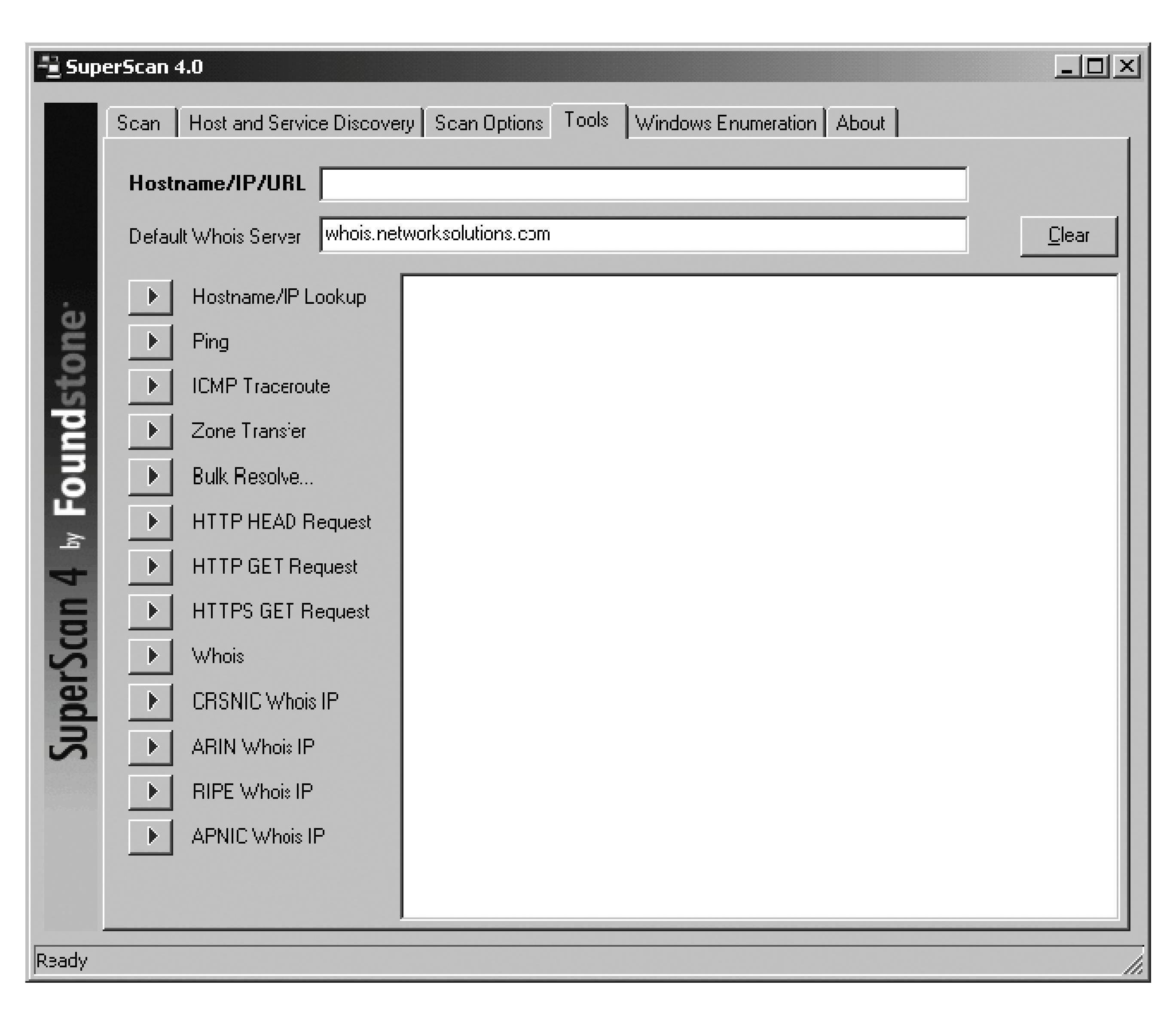


图 8.24　Tools 选项卡

第 5 步 使用 Windows 枚举选项。

最后的功能选项是 Windows 枚举选项，就像用户大概猜测的一样，如果用户设法收集的信息是关于 Linux/UNIX 主机的，那这个选项是没什么用的。但若用户需要 Windows 主机的信息，它确实是很方便的。如图 8.25 所示，其中能够提供从单个主机到用户群组，再到协议策略的所有信息。

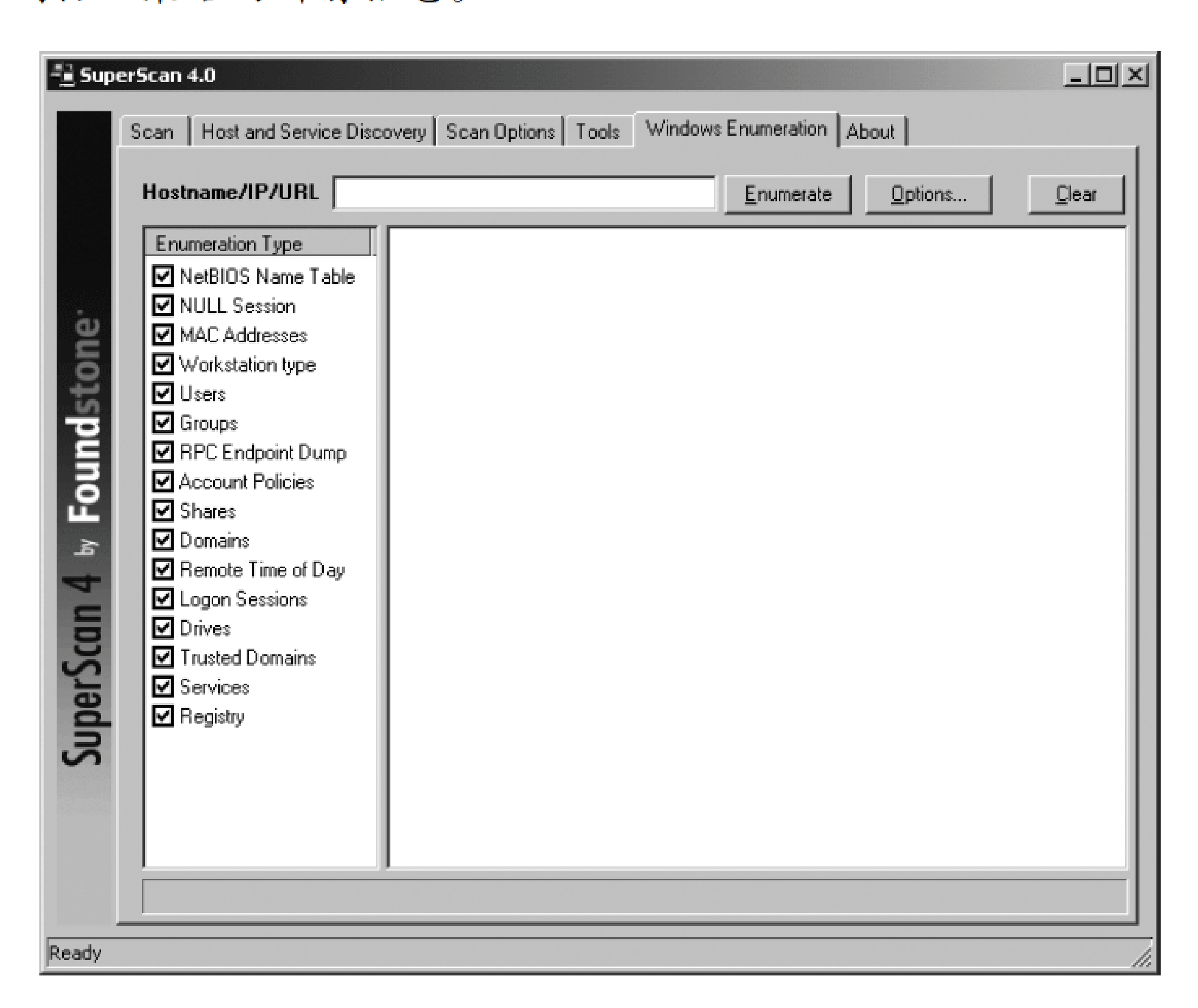


图 8.25 Windows 枚举选项

8.4.3 网络监听工具

网络监听是一种常用的被动式网络攻击方法，能帮助入侵者轻易获得用其他方法很难获得的信息，包括用户口令、账号、敏感数据、IP 地址、路由信息、TCP 套接字号等。类似"食肉动物"一类的监听软件，一旦成功地登录目标网络上的一台主机，就会取得该机的超级用户权限，而且往往会尝试攻击网络中的其他主机，以实现对整个网络的监听。

网络监听通常在网络接口处截获计算机之间通信的数据流，是进行网络攻击最简单、最有效的方法，它具有以下特点。

(1) 隐蔽性强。进行网络监听的主机只是被动地接收网上传输的信息，没有任何主动的行为，既不修改网上传输的数据包，也不往链路上插入任何数据，很难被网络管理员觉察到。

(2) 手段灵活。网络监听可以在网上的任何位置实施，可以是网上的一台主机、路由器，也可以是调制解调器。其中，网络监听效果最好的地方是在网络中某些具有战略意义的位置，如网关、路由器、防火墙之类的设备或重要网段；而使用最方便的地方是在网中的一台主机上。

正因为网络监听具有以上特点，因此检测非常困难，这意味着更大的安全危害。虽然成功检测到网络监听难度很大，但网络监听并非无懈可击，通过采取积极、有效的措施，就

能够发现它的蛛丝马迹。

监听非常消耗 CPU 资源，当系统运行网络监听软件时，系统因负荷过重，而对外界的响应很慢。因此，对于怀疑运行监听程序的主机，可用正确的 IP 地址和错误的物理地址去探测（如 Ping），运行监听程序的主机会有响应。这是因为正常的主机不接收错误的物理地址，而处于监听状态的主机能接收。另外，可向网上发送大量目的地址根本不存在的数据包，由于监听程序将处理这些数据包，会导致主机性能下降。通过比较该主机前后的性能，就可以作出判断，但这种方法难度较大。当前，有两个比较可行的办法：一是搜索网上所有主机运行的进程。网络管理员使用 UNIX 或 Windows NT 的主机，可以很容易地得到当前进程的清单，并确定是否有一个进程被从管理员主机上启动；二是搜查监听程序。现在监听程序只有有限的几种，管理员可以检查目录，找出监听程序。

还有两个方法在发现监听方面比较有效，但缺点是难度较大：一是检查被怀疑主机中是否有一个随时间不断增长的文件存在，因为网络监听输出的文件通常很大，且随时间不断增长；二是通过运行 Ipconfig 命令检查网卡是否被设置成了监听模式，或使用 Ifstatus 工具，定期检测网络接口是否处于监听状态。当网络接口处于监听状态时，很可能是入侵网络监听的防范一般比较困难，通常可采取数据加密和网络分段两种方法。

（1）数据加密。数据加密的优越性在于，即使攻击者获得了数据，如果不能破译，这些数据对他也是没有用的。一般而言，人们真正关心的是那些秘密数据的安全传输，使其不被监听和偷换。如果这些信息以明文的形式传输，就很容易被截获而且阅读出来。因此，对秘密数据进行加密传输是一个很好的办法。

（2）网络分段。即采用网络分段技术，建立安全的网络拓扑结构，将一个大的网络分成若干个小的网络，如将一个部门、一个办公室等可以相互信任的主机放在一个物理网段上，网段之间再通过网桥、交换机或路由器相连，实现相互隔离。这样，即使某个网段被监听了，网络中其他网段还是安全的。因为数据包只能在该子网的网段内被截获，网络中剩余的部分（不在同一网段的部分）则被保护了。

8.4.4 木马程序

一般的木马程序都有客户端和服务器端两个执行程序，其中客户端是用于黑客远程控制植入木马的机器的程序，服务器程序即是木马程序。如果黑客要通过木马入侵用户的系统，他所要做的第一步就是要让木马的服务器端程序在用户的计算机中运行。一旦运行成功，木马程序就可以获得系统管理员的权限，在用户毫不觉察的情况下，对计算机做任何能做的事情，所以，计算机用户应该经常检查自己的系统，做好木马的预防和清除工作。下面以国产的木马程序冰河为例。

冰河是一个优秀的木马程序，它功能众多，几乎涵盖了所有的 Windows 的常用操作，并具有简单、明了的中文使用界面。

冰河的服务器端和客户端都是一个可执行的文件。服务器程序在目标计算机上执行以后，该计算机的 7626 号端口就对外开放了。如果在客户端输入其 IP 地址，就可完全控制这台计算机了，图 8.26 所示为冰河程序的客户端窗口。

其主要功能及特点如下。



图 8.26 冰河 V8.4 的客户端窗口

(1) 记录各种口令信息。它包括开机口令、屏保口令、共享资源口令等,随着版本的升高,它所能够记录的口令信息会增加。

(2) 获取系统信息。它主要包括计算机名、当前用户、系统路径、操作系统版本、物理及逻辑磁盘信息等多项系统数据。

(3) 远程文件操作。可以进行创建、上传、下载、复制、删除文件,文件压缩、远程打开文件等多种文件操作功能。

(4) 限制系统功能。它具有远程关机、远程重启机器、锁定鼠标、启用热键等功能。

(5) 发送信息。这是指向被控端发送短信息。

(6) 注册表操作。它包括对主键的浏览、增删、复制等操作。

(7) 点到点通信。以聊天室的形式同被控制端进行在线交谈。

8.5 黑客攻击的防范

8.5.1 防止黑客攻击的措施

各种黑客的攻击程序虽然功能强大,但并不可怕。只要我们做好相应的防范工作,就可以大大降低被黑客攻击的可能性。具体来说,要做到以下几点。

1. 要提高安全意识

不随意打开来历不明的电子邮件及文件,不随便运行不太了解的人送给的程序,防止运行黑客的服务器程序。尽量避免从 Internet 下载不知名的软件和游戏程序。即使从知名的网站下载的软件也要及时用最新的病毒和木马查杀工具对软件和系统进行扫描。密码设置尽量能使用字母数字混排,单纯的英文或者数字很容易被破解。常用的若干密码不应设置成相同的内容,密码最好经常更换。要及时下载并安装系统补丁程序。不随便运行黑客程序。

2. 使用反黑客软件

尽可能经常性地使用多种最新的、能够查解黑客的杀毒软件或可靠的反黑客软件来检查系统。必要时应在系统中安装具有实时检测、拦截、查解黑客攻击程序的工具。

3. 使用防火墙

防火墙是抵御黑客程序入侵的非常有效的手段。它通过在网络边界上建立起来的相应网络通信监控系统来隔离内部和外部网络，可阻挡外部网络的入侵和攻击。

4. 安装杀毒软件

要将防毒、防黑当成日常例行工作，定时更新防毒组件，及时升级病毒库，将防毒软件保持在常驻状态，以彻底防毒。

5. 做好数据的备份

确保重要数据不被破坏的最好办法就是定期或不定期的备份数据，特别重要的数据应该每天备份。

6. 隐藏自己的 IP

保护自己的 IP 地址是很重要的。事实上，即便用户的机器上被安装了木马程序，若没有用户的 IP 地址，攻击者也是没有办法的，而保护 IP 地址的最好方法就是设置代理服务器。代理服务器能起到外部网络申请访问内部网络的中间转接作用，其功能类似于一个数据转发器，它主要控制哪些用户能访问哪些服务类型。

总之，我们应当认真制定有针对性的策略。明确安全对象，设置强有力的安全保障体系。在系统中层层设防，使每一层都成为一道关卡，从而让攻击者无隙可钻、无计可施。

8.5.2 发现黑客入侵后的对策

1. 估计受害形势，发出攻击警报

当确认系统受到入侵时，首先应尽可能快地估计出入侵造成的破坏程度。当系统遇到严重破坏或不能正常运行时，应向相关公安部门和信息安全管理部门报告，以便通过司法手段解决问题。

2. 采取措施

(1) 杀死这个进程以切断黑客与系统的连接。必要时，切断网络连接，同时，注意保存现场，以便事后调查原因并进行分析。

(2) 使用安全工具跟踪这个连接，找出黑客的来路和身份，询问他们究竟想要做什么，并发出警告。

(3) 管理员可以使用一些工具来监视黑客，观察他们在做什么。

3. 使用网络工具

可以通过网络安全工具找到入侵者从哪个主机过来,然后查看哪些用户登录进入远程系统。

4. 修复漏洞

修复安全漏洞并恢复系统,不给黑客可乘之机。



【案例】"灰鸽子"的清除与防范

案例分析

为了使"灰鸽子"避开杀毒软件的查杀,有些人就会故意给"灰鸽子"加上各种不同的壳,造成网络上不断有新的"灰鸽子"变种出现。即便是有杀毒软件,也难免会有一些"漏网之鱼"。如果机器中出现了"灰鸽子"症状,但杀毒软件查杀不到,就很有可能是机器被感染了还没有被截获的新变种。这个时候,就需要手工清除掉"灰鸽子"。手工清除"灰鸽子"并不难,重要的是必须懂得它的运行原理。

1. "灰鸽子"的运行原理

"灰鸽子"远程监控软件分为两部分:客户端和服务器端。黑客操纵着客户端,利用客户端配置生成一个服务器端程序。服务器端文件的名字默认为 G-Server. exe 运行之后,会将自己拷贝到 Windows 文件夹下,再释放 G-Server. dll 和 G-Server-HOOK. dll 到 Windows 文件夹下。G-Server. exe、G-Server. dll、G-Server- HOOK. dll 这 3 个文件夹互相配合组成了"灰鸽子"服务器端,有些还会多释放出一个名为 G-ServerKey. dll 的文件夹用来记录键盘操作。

Windows 文件夹下的 G-Server. exe 文件会将自己注册成服务状态,这样,用户在每次开机之后都将自动运行该文件,启动 G-Server. dll 和 G-Server-Hook. dll 并自动退出。

G-Server. dll 文件可实现后门功能,与客户端进行通信;G-Server-Hook. dll 则通过拦截 API 调用来隐藏病毒。因此,用户在中毒之后既看不到病毒文件,也看不到病毒注册的服务项,随着"灰鸽子"服务器端文件的设置不同,G-Server-Hook. dll 有时会附在 Explorer. exe 的进程空间中,有时则是附在所有进程中。

2. "灰鸽子"的手工检测

由于"灰鸽子"拦截了 API 调用,在正常模式下服务器端程序文件和其注册的服务项均被隐藏,也就是说,用户即使设置了"显示所有隐藏文件"也看不到它们。此外,"灰鸽子"服务器端的文件名也是可以自定义的,这都给手工检测带来了一定的困难。

但仔细观察后就会发现,无论自定义的服务器端文件名是什么,一般都会在操作系统的安装目录下生成一个以"-hook. dll"结尾的文件。通过这一点,即可较为准确地手工检测出"灰鸽子"的服务器端。

由于正常模式下"灰鸽子"会隐藏自身,因此检测"灰鸽子"的操作一定要在安全模式下进行。

操作环境

Windows Server 2003 操作系统。

操作步骤

第 1 步 在系统启动并进入 Windows 启动画面前，按 F8 键(或在启动计算机时按住 Ctrl 键)，在出现的启动选项菜单中，选择 Safe Mode 或“安全模式”启动项。

第 2 步 由于“灰鸽子”的文件本身具有隐藏属性，因此，要设置 Windows 显示所有文件。在“我的电脑”窗口中选择“工具”→“文件夹选项”命令，即可打开“文件夹选项”对话框。

第 3 步 在“查看”选项卡中取消选中“隐藏受保护的操作系统文件”复选框，并在“隐藏文件和文件夹”选项组中选中“显示所有文件和文件夹”复选框。

第 4 步 打开 Windows 的搜索文件功能，在文件名称框中输入“*_hook.dll”，搜索位置选择 Windows 的安装文件夹。

第 5 步 单击“搜索”按钮，即可在 Windows 文件夹下发现“灰鸽子”的木马程序文件，如 Game_Hook.dll 文件。

第 6 步 根据“灰鸽子”原理分析可知，如果 Game_Hook.dll 是“灰鸽子”的文件，则在操作系统安装文件夹下还会有 Game.exe 文件和 Game.dll 文件。打开 Windows 文件夹，可查找到这两个文件，同时还有一个用于记录键盘操作的 GameKey.dll 文件。

在经过上述操作之后，基本上就可以确定这些文件是“灰鸽子”服务器端程序，下面就可以对其进行手动清除了。

清除“灰鸽子”仍然要在安全模式下操作，主要有两步：清除“灰鸽子”的服务；删除“灰鸽子”程序文件。清除“灰鸽子”的服务一定要在注册表里完成，对注册表不熟悉的用户请找熟悉的朋友帮忙操作。清除“灰鸽子”的服务之前，为防止操作失误而引起的麻烦，一定要先备份注册表，或者到纯 DoS 下将注册表文件更名之后，再去注册表删除“灰鸽子”的服务(因为病毒会在.exe 文件中进行关联)。

清除“灰鸽子”服务的具体操作步骤如下。

第 7 步 在注册表编辑中，展开到[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSer\Setvices]注册表项。

第 8 步 选择“编辑”→“查找”命令，即可打开“查找”对话框，在“查找目标”文本框中输入“game.exe”。

第 9 步 单击“查找下一个”按钮，即可找到“灰鸽子”的服务项(此例为 Game_Server)，删除整个 Game_Hook.dll 及 Gamekey.dll 文件之后，重新启动计算机即可。至此，“灰鸽子”服务器端程序就被彻底清除干净了。

上述方法适用于大部分“灰鸽子”木马及其变种，但仍有极少数变种采用此方法无法检测和清除。同时，随着“灰鸽子”新版本的不断推出，手工检测和清除“灰鸽子”的难度也会越来越大。

本 章 小 结

黑客是指那些利用计算机技术及其他手段，善意或恶意地进入非授权范围内的计算机或网络空间的人。

黑客攻击的目的主要有获取目标系统的非法访问、获取所需资料、篡改有关数据及利用有关资源。黑客的攻击手段包括特洛伊木马攻击、Web 欺骗、口令攻击、缓冲区溢出、端口扫描攻击等几种主要的方法。对常见攻击方法的了解，将有助于用户达到有效防黑的目的。

掌握常见的木马程序、扫描工具、破解工具、炸弹工具及安全防御工具的特点和使用方法，做好相应的防黑措施，设置强有力的安全保障体系，就可以大大降低被黑客攻击的可能性。

本 章 练 习

一、填空题

1. 通常黑客攻击的三个阶段是________、________和________。
2. 常见的黑客攻击方法有________、________、________、________、________、________等。
3. 特洛伊木马是一种黑客程序，它一般包括两个程序：一个是________；另一个是________。
4. 传播木马的方式主要有两种：一种是________；另一种是________。
5. 扫描工具是________的程序。

二、选择题

1. 如果每次打开 Word 程序编辑文档时，计算机都会把文档传送到一台 FTP 服务器，那么可以怀疑 Word 程序已经被黑客植入________。

   A. 蠕虫　　B. FTP 程序　　C. 特洛伊木马　　D. 陷门

2. 以下网络攻击中，________不属于主动攻击。

   A. 重放攻击　　B. 拒绝服务攻击
   C. 通信量分析攻击　　D. 假冒攻击

3. 有一种攻击是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，这种攻击叫作________。

   A. 重放攻击　　B. 反射攻击
   C. 拒绝服务攻击　　D. 服务攻击

4. ________不属于防止口令猜测的措施。

   A. 严格限定从一个给定的终端进行非法认证的次数

B. 确保口令不在终端上再现

C. 防止用户使用太短的口令

D. 使用机器产生的口令

5. 在网络安全中，截取是指未授权的实体得到了资源的访问权，这是对________。

A. 可用性的攻击　　　　B. 完整性的攻击

C. 保密性的攻击　　　　D. 真实性的攻击

三、简答题

1. 什么是黑客？
2. 黑客攻击的目的是什么？
3. 简述黑客攻击的步骤。
4. 列举一些黑客攻击所采用的方法，并做简单分析。
5. 常见的木马工具有哪些？它们是怎样运行的？
6. 在使用计算机时，应采取哪些防黑措施？

实训　冰河木马分析与清除

实训目的

（1）了解远程控制的基本原理。

（2）熟悉冰河木马的功能。

实训环境

（1）一台可以连上 Internet 的计算机。

（2）Windows 2003/XP 操作系统。

实训步骤

第 1 步　安装并控制远程目标。

安装冰河木马，并将冰河木马服务器端植入目标计算机。

第 2 步　跟踪目标。

通过服务器端自动跟踪目标机屏幕变化同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕上（局域网适用）。

第 3 步　记录各种口令信息。

这些口令信息包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息。

第 4 步　获取系统信息。

这些系统信息包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显

示分辨率、物理及逻辑磁盘信息等多项系统数据。

第 5 步 远程文件操作。

远程文件操作包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件等多项文件操作功能。

第 6 步 注册表操作。

注册表操作包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。

第 7 步 发送信息。

以 4 种常用图标向被控端发送简短信息。

第 8 步 冰河木马的清除。

(1) 冰河控制端可以自动卸载。

(2) 手动清除方法：删除注册表中 Kernel32. exe 的键值；修改相关文本文件的关联；在 DoS 模式下将 Sysexplr. exe 和 Kernel32. exe 的隐藏属性改为只读，然后删除它们。

第 9 章

Web 安全技术

Chapter 9

知识目标

- 了解 HTTP 协议、HTML 语言。
- 掌握服务器的安全策略。
- 掌握浏览器、服务器的安全问题。

技能目标

- 能够对服务器进行基本的安全配置。
- 能够对浏览器进行安全配置。

Web 作为 Internet 的一项重要的应用被广泛使用,它的安全性是必须要考虑的问题。

9.1 Web 技术简介

万维网(world wide web,WWW)是 Internet 上发展最快同时又使用最多的一项服务,它可以提供包括文本、图形、声音和视频等在内的多媒体信息。

WWW 起源于 1989 年欧洲粒子物理研究所(CERN)。其目的是收集时刻变化的报告,蓝图、绘制图、照片和其他文献。链接文档的 Web 的最初计划是由 CERN 的物理学家 Tim Bermers-Lee 于 1989 年 3 月提出的,第一个原型(基于文本的)于 18 个月后运行。1991 年 12 月在得克萨斯州的圣安东尼奥(San Antonio)91 超文本会议上进行了一次公开演示,次年继续发展,并于 1993 年 2 月,在第一个图形界面 Mosaic 的发布时达到了其发展的高峰。到今天 WWW 已经成为 Internet 上不可缺少的技术。

9.1.1 Web 基础知识

WWW 由遍布 Internet 中的被称为 WWW 服务器(又称为 Web 服务器)的计算机组成。Web 是一个容纳各种类型信息的集合,从用户的角度看,WWW 由庞大的、世界范围的文档集合而成,简称为页面。页面具有严格的格式,页面是用超文本标识语言(hyper text markup language,HTML)写成的,存放在 Web 服务器上。每一页面可以包含到世界上任何地方的其他相关页面的超链接(hyperlink),这种能够指向其他页面的页称为超

文本(hypertext)。用户可以跟随一个超链接到其所指向的其他页面,并且这一过程可以被无限制的重复。通过这种方法可浏览无数的互相链接的信息。

用户使用浏览器总是从访问某个主页开始的。由于页中包含了超链接,因此可以指向另外的页,这样就可以查看大量的信息。下面我们来看一下 WWW 中常用的一些术语及其意义。

1. HTML

HTML 是 ISO 标准 8879 标准通用标识语言(standard generalized markup language,SGML)在 WWW 上的应用。所谓标识语言,就是格式化的语言,存在于 WWW 服务上的页,就是用 HTML 描述的,它使用一些约定的标记对 WWW 的包括文字、声音、图像、视频等各种信息及超级链接进行描述。当用户浏览 WWW 上的信息时,浏览器会自动地解释这些标记的含义,并将其显示为用户在屏幕上所看到的网页。

一个 HTML 文本包括文件头(Head)、文件(Body)主体两部分,其结构如下。

```
<HTML>
<HEAD>

</HEAD>
<BODY>

</BODY>
</HTML>
```

其中,<HTML>表示页的开始,</HTML>表示页的结束,它们是成对使用的。<HEAD>表示头开始,</HEAD>表示头结束;<BODY>表示主体开始,</BODY>表示主体结束,它们之间的内容才会在浏览器的正文中显示出来。HTML 的标识符有很多,可以查看有关网页制作方法的书籍。

2. 超文本传输协议

超文本传输协议(hypertext transfer protocal,HTTP)是用来浏览器和 WWW 服务器之间传达超文本的协议。HTTP 协议由两个相当明显的项组成:从浏览器到服务器的请求集和从服务器到浏览器的应答集。HTTP 协议是一种面向对象的协议,为了保证 WWW 客户机与 WWW 服务器之间通信不会产生二义性,HTTP 精确定义了请求报文和响应报文的格式。HTTP 会话过程包括 4 个步骤:连接、请求、应答和关闭。

3. 统一资源定位器

WWW 是以页面的形式来组织信息的。那么怎样来识别不同的页面,怎样才能知道页面在哪个位置,以及如何访问页面呢?为了解决这个问题,WWW 采用了统一资源定位器(uniform resource locator,URL)的方法。

URL 是在 Internet 上唯一确定资源位置的方法,其基本格式为:

协议://主机域名/资源文件名

其中,协议(protocal)用来指明资源类型,除了 WWW 用的 HTTP 协议之外,还可以是 FTP、Telnet 等;主机域名表示资源所在机器的 DNS 名字;资源文件名用以提出资源在所在机器上的位置,包含路径和文件名,通常是"目录名/目录名/文件名",也可以不含有路径。例如,新浪网的 WWW 主页的 URL 就表示为 http://www.sina.com.cn/index.htm。

在输入 URL 时,资源类型和服务器地址不分字母的大小写,但目录和文件名则可能区分字母的大小写。这是因为大多数服务器安装了 UNIX 操作系统,而 UNIX 的文件系统是区分文件名的大小写的。

9.1.2 Web服务器

Internet 上众多的 Web 服务器汇集了大量的信息,Web 服务器的作用就是管理这些文档,处理用户发来的各种请求,将满足用户要求的信息返回给用户。

其实,本质上来说,Web 服务器是驻留在服务器上的一个程序,通过 Web 浏览器与用户交互操作,为用户提供相关信息。

9.1.3 Web浏览器

Web 浏览器是阅读 Web 上信息的客户端的软件。如果用户在本地机器上安装了 Web 浏览器软件,就可以读取 Web 上的信息了。

Web 浏览器在网络上与 Web 服务器打交道,从服务器上下载和获取文件。Web 浏览器有多种,它们都可以浏览 Web 上的内容,只不过所支持的协议标准及功能特性各有异同罢了。绝大部分的浏览器都运用了图形用户界面。目前常用的有 Microsoft Internet Explorer Opera 和 Lynx 等。

9.2 Web 的安全风险

9.2.1 Web的安全体系结构

Web 的安全有很多因素需要考虑,如 Web 服务器的安全、Web 服务器所在网络的安全、Web 浏览器无辜用户的安全风险等。

Web 的安全体系结构非常复杂,具体来说,包括以下几个方面。

(1) Web 浏览器软件的安全。

(2) Web 服务器上 Web 服务器软件的安全。

(3) 主机系统的安全。

(4) 客户端局域网的安全。

(5) 服务器端局域网的安全。

(6) Internet 的安全。

所有以上因素必须考虑在内,才能说是较好地分析了 Web 系统的安全性。

9.2.2 Web服务器的安全风险

现在,随着开放系统的发展和 Internet 的延伸,技术间的交流变得越来越容易,同时,人们也更容易获取功能强大的攻击安全系统的工具软件;另外,由于人才流动频繁,掌握系统安全情况的有关人员可能会成为无关人员,从而使得系统安全秘密扩散的成为可能。

Web 服务器的安全风险主要来自以下几个方面。

(1) 能否保证公布信息的真实、完整

维护公布的信息的真实性和完整性是 Web 服务器最基本的要求。Web 服务器在一定程度上是站点拥有者的代言人,代表拥有者的形象。如果公布的信息被人篡改,可能会使得信息遭到破坏,无法真正提供信息服务,甚至会导致用户和站点拥有者的矛盾或者影响站点的形象。

(2) Web 服务能否安全、可用

由于系统本身可能出现的问题及他人恶意的破坏,可能会造成用户不能够获得 Web 服务,或者不能保证 Web 的服务确实有效;另外,需要保证所提供的服务是可信的,尤其是金融或者电子商务的站点。

(3) 能否很好地保证 Web 访问者的隐私

要想取得用户的信赖,放心使用 Web 服务器的前提,首先要保护 Web 访问者的隐私。服务器上一般保留着用户的个人信息,如用户 IP 地址、电子邮件地址、所用计算机名称、单位名称、计算机简单说明、所访问页面内容、访问时间、传输数据量,甚至个人的信用卡号码等信息。一般情况下,用户不希望自己的隐私被别人发现甚至利用。

(4) Web 服务器可能会被入侵者作为“跳板”使用

这是 Web 服务器最基本的要求。是服务器保护自己和 Web 浏览器用户的最基本的条件。但常有非法入侵者将 Web 服务器作为“跳板”使用来进一步侵入内部网络或进一步危害其他网络。

9.2.3 Web浏览器的安全风险

Web 浏览器为用户提供了一个功能强大、简单实用的图形化的界面,使用户不必经过专业化训练就可轻松自如地在网络的海洋里冲浪。它是目前网络上应用得最多的工具之一。但使用 Web 浏览器获取信息时,也是有安全风险的,主要有以下几个方面。

(1) 运行浏览器的系统可能会被病毒或者其他恶意程序侵害而遭受破坏。

(2) 个人信息可能会外泄。

(3) 不能确保所交互的站点的真实性,用户可能会受骗,受到损失。

例如,某浏览器的用户轻点鼠标,想要看看新闻,查找一下资料,浏览一下某公司的主页,当一张张精彩的网页出现在计算机屏幕上时,同时,浏览器程序可能已经把某些信息传送给网络上的某一台计算机,这台计算机可能在世界的另一个角落,网页通过网络传到浏览器计算机中的时候,传来的内容有的是浏览器用户需要的、能够看到的,但是同时还有浏览器不能显示的内容,悄悄地存入浏览器计算机的硬盘上,这些不显示的内容,可能是协议工作内容,对用户是透明的,但是也可能是恶作剧代码,或者是蓄意破坏的代码,它

们会窃取 Web 浏览器用户的计算机上的所有可能的隐私，也可能破坏计算机的设备，不可能使得用户在上网时误入歧途。因此，Web 浏览器也是有安全风险的。

9.3　Web 浏览器的安全

如果所有的网络用户都能够安分地使用网络这个美好的工具，那么 Web 浏览器用户就没有什么可以担忧的了，但非常不幸的是，网络世界是良莠不齐、复杂多样的，可能随时会受到恶意的攻击甚至被毁坏。

9.3.1　浏览器本身的漏洞

浏览器的功能越来越强大，但是由于程序结构的复杂，在堵住了旧的漏洞的同时，可能又出现了新的漏洞。浏览器的安全漏洞可能让攻击者获取磁盘信息、安全口令，甚至破坏磁盘文件系统等。下面举出两个已知的浏览器安全漏洞。

1. UNIX 下 Lynx 的安全漏洞

在 Lynx 的 2.7.1 版本之前都存在安全漏洞，只要做一个包含 backtick 字符的 LynxDownLoadURL，它就允许 Web 创建者在用户的机器上执行任意命令。解决这个问题的方法是升级 Lynx 的版本。

2. Microsoft Internet Explorer 的安全威胁

在这个浏览器中存在着许多安全威胁。

(1) 远程执行代码漏洞

在 Microsoft Internet Explorer 8.0 或 9.0 版本，Internet Explorer 访问内存中已被删除或尚未正确分配的对象的方式中存在一个远程执行代码漏洞。该漏洞可能以一种允许攻击者在 Internet Explorer 中的当前用户的上下文中执行任意代码的方式损坏内存。攻击者可能拥有一个旨在通过 Internet Explorer 利用此漏洞的特制网站，然后诱使用户查看该网站。解决的方法就是安装补丁程序或者升级浏览器版本。

(2) 拒绝服务漏洞

Microsoft Internet Explorer 8.0 处理恶意脚本代码存在问题，远程攻击者可以利用漏洞使应用程序崩溃。通过构建恶意 Web 页，诱使用户访问可触发此漏洞。

(3) 地址栏 URI 欺骗漏洞

在 Microsoft Internet Explorer 8.0 或 9.0 版本代理服务设置中，如果 HTTP 和 Secure 栏中具有相同代理地址和端口，IE 没有确保 SSL 锁定图标与地址栏一致，通过特制的 HTML 文档触发多个任意主机的 HTTPS 请求，随后提交一个可信主机的 HTTPS 请求，再向不可信主机发送一个 HTTP 请求，可欺骗 Web 站点。

(4) Singapore 隐私漏洞

它允许一个网络黑客监视用户在 Web 上的活动。使用最新版本的浏览器可以避免这个漏洞。

当然,可能有许多的漏洞还没发现。

9.3.2 Web 页面中的恶意代码

由于某些动态页面以来源不可信的用户输入的数据为参数生成页面,所以 Web 页面中可能会不经意地包含一些恶意的脚本程序等。如果 Web 服务器不对此进行处理,那么很可能对 Web 服务器和浏览器用户两方面都带来安全威胁。即使采用 SSL 来保护传输,也不能阻止这些恶意代码的传输。

9.3.3 Web 欺骗

由于 Internet 上 Web 网页容易复制的特点,使得 Web 欺骗变得简单。

1. 欺骗攻击

所谓欺骗攻击,就是指攻击者通过伪造一些容易引起错觉的文件、音像或者其他场景来诱导受骗者做出错误的与安全有关的决策。在网络虚拟的世界里,同样存在被骗的受害者。Web 欺骗就是一种网络欺骗,攻击者构建的虚假网站看起来就像真实站点,具有同样的连接,同样的页面,而实际上,被欺骗的所有浏览器用户与这些伪装的页面的交互过程都受到攻击者控制。

2. Web 欺骗攻击的原理

Web 欺骗攻击成功的关键在于攻击者的伪服务器必须位于受骗用户到目标 Web 服务的必经的路径上。

攻击者首先在某些 Web 网页上改写所有与目标 Web 站点有关的链接,使得不能指向真正的 Web 服务器,而是指向攻击者的伪服务器。当用户单击这些链接时,首先指向了伪服务器,攻击者向真正的服务器索取用户的所需界面。当获得目标 Web 送来的页面后,伪服务器改写链接并加入伪装代码,送给被欺骗的浏览器用户。

3. 对策

Web 欺骗攻击的危害大,上当的用户可能会不知不觉泄露机密信息,还可能受到经济损失。为确保安全,用户可以采取的措施如下。

(1) 尽量避免非有不可的浏览器的 JavaScript、ActiveX 和 Java 选项。

(2) 充分利用浏览器的提示信息。

(3) 进入 SSL 安全链接时,仔细查看站点的证书是否与其所声称的一致,不要被相似的字符欺骗。



【案例】 Web浏览器的安全设置

案例分析

在 IE 浏览器中，有一些安全设置的功能，根据安全需求正确地进行设置，可以帮助我们提高浏览网页时的安全性。

操作环境

(1) 一台连上 Internet 的计算机。

(2) IE 8.0 浏览器。

操作步骤

第 1 步　Web 浏览器的安全设置。

(1) 打开 IE 8.0 浏览器，在“工具”菜单中选择“Internet 选项”命令，打开“安全”选项卡，如图 9.1 所示。

(2) 单击“自定义级别”按钮，弹出“安全设置-Internet 区域”对话框，如图 9.2 所示。



图 9.1　“安全”选项卡



图 9.2　“安全设置”对话框

(3) 在“重置自定义设置”选项值中的“重置为”下拉列表中选择需要更改的安全级别，然后单击“重置”按钮，弹出“警告!”对话框，如图 9.3 所示。单击“是”按钮，就重置了安全设置。

第 2 步　IE 浏览器中的 ActiveX 设置。

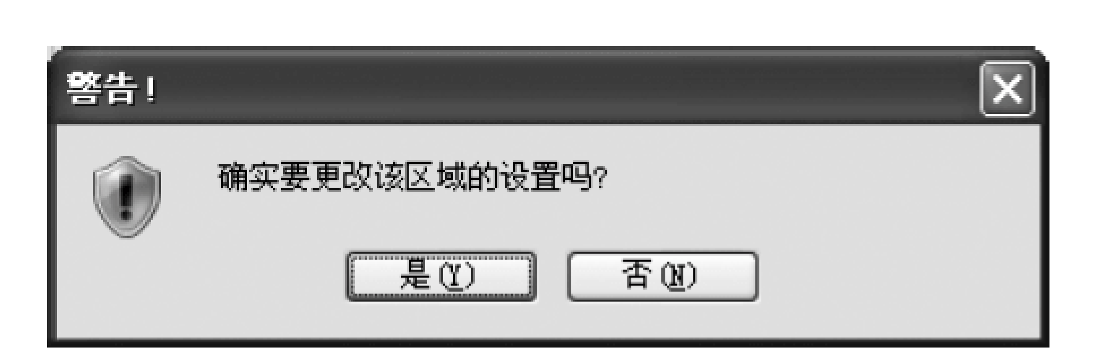


图 9.3 “警告!”对话框

第 3 步 定期清除用户信息。

(1) 单击“Internet 选项”对话框→“内容”选项卡,如图 9.4 所示,单击“自动完成”选项组的“设置”按钮。

(2) 打开“自动完成设置”对话框,选中“自动完成功能应用于”选项组中的“表单”复选框,如图 9.5 所示。

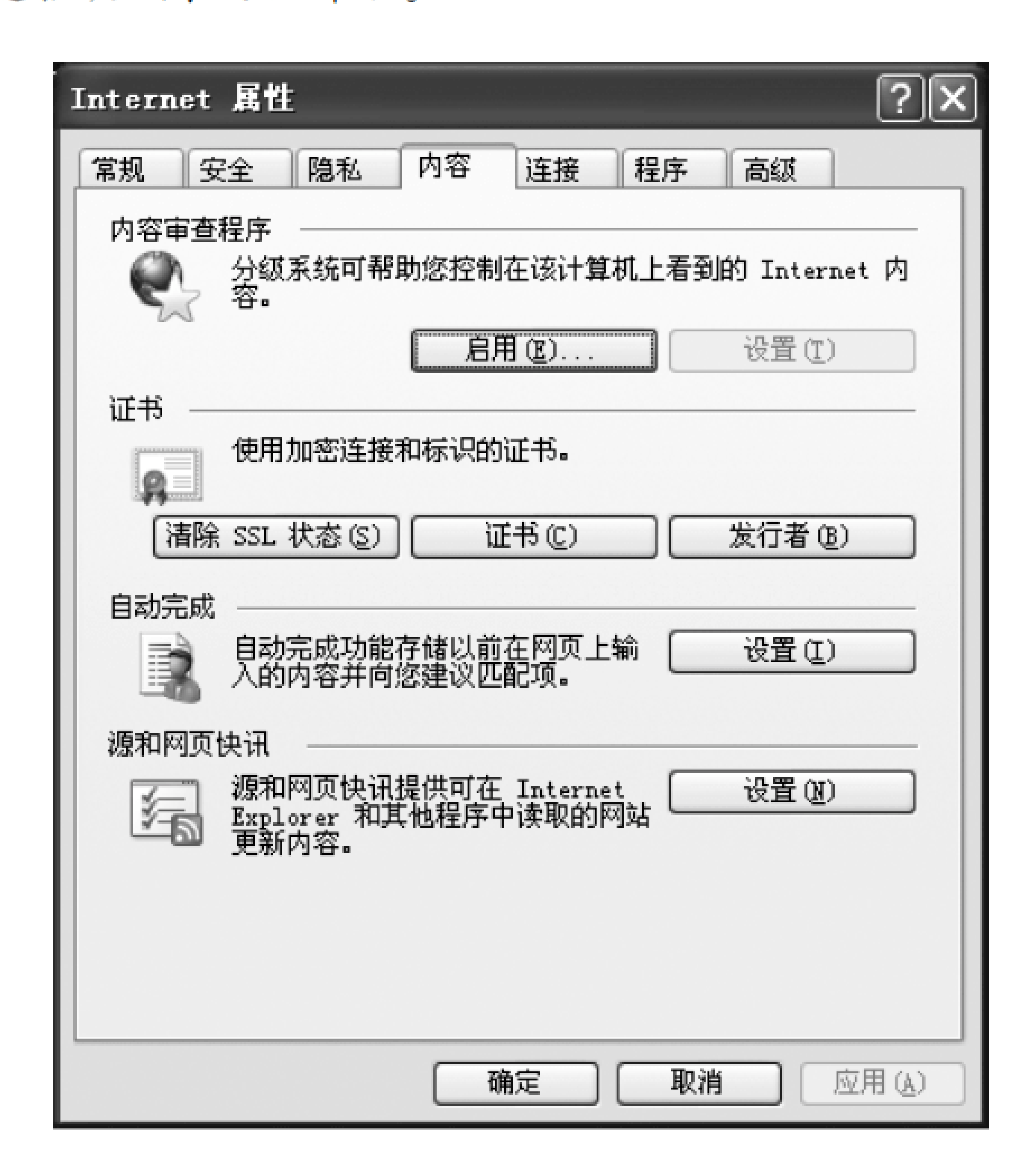


图 9.4 “内容”选项卡

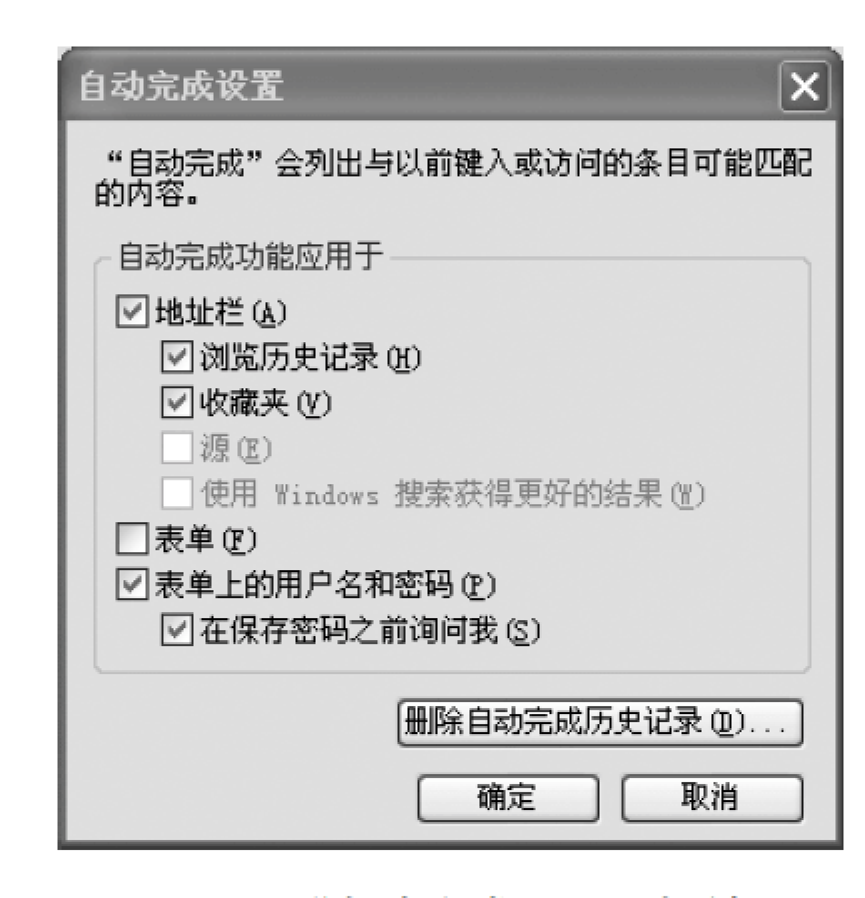


图 9.5 “自动完成设置”对话框

(3) 单击“删除自动完成历史记录”按钮可以清除历史记录。

第 4 步 对 IE 中数据执行保护设置。

(1) 右击“我的电脑”,在弹出的快捷菜单中选择“属性”菜单,打开“系统属性”对话框,如图 9.6 所示,选择“高级”选项卡。

(2) 单击“性能”区域中的“设置”按钮,打开“性能选项”对话框,打开“数据执行保护”选项卡,如图 9.7 所示,单击“应用”按钮,保存即可。

第 5 步 分级审查。

(1) 打开“Internet 属性”对话框的“内容”选项卡,如图 9.8 所示。

(2) 在“内容审查程序”选项组中单击“启用”按钮。




图 9.6 "系统属性"对话框



图 9.7 "数据执行保护"选项卡

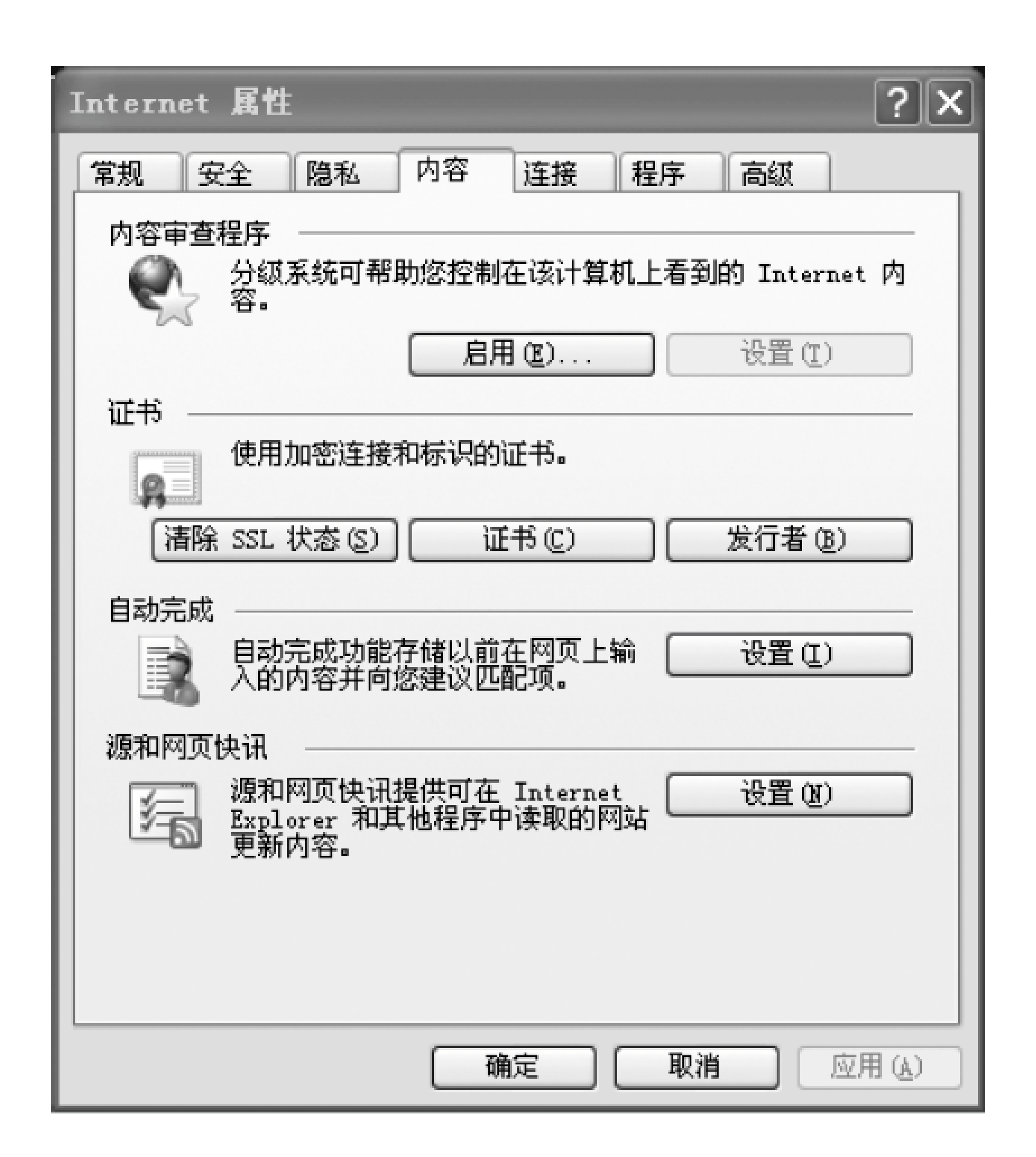


图 9.8 "内容"选项卡

(3) 在弹出的"内容审查程序"对话框中，如图 9.9 所示，打开"分级"选项卡，将调整分级级别的滑块调到最低，也就是零。

(4) 打开"许可站点"选项卡，如图 9.10 所示，在"允许该网站"文本框中添加网站。

(5) 打开"常规"选项卡，如图 9.11 所示，单击"创建密码"按钮，打开"创建监护人密码"对话框，在此创建监护人密码，如图 9.12 所示。



图 9.9 “内容审查程序”对话框



图 9.10 “许可站点”选项卡



图 9.11 “常规”选项卡

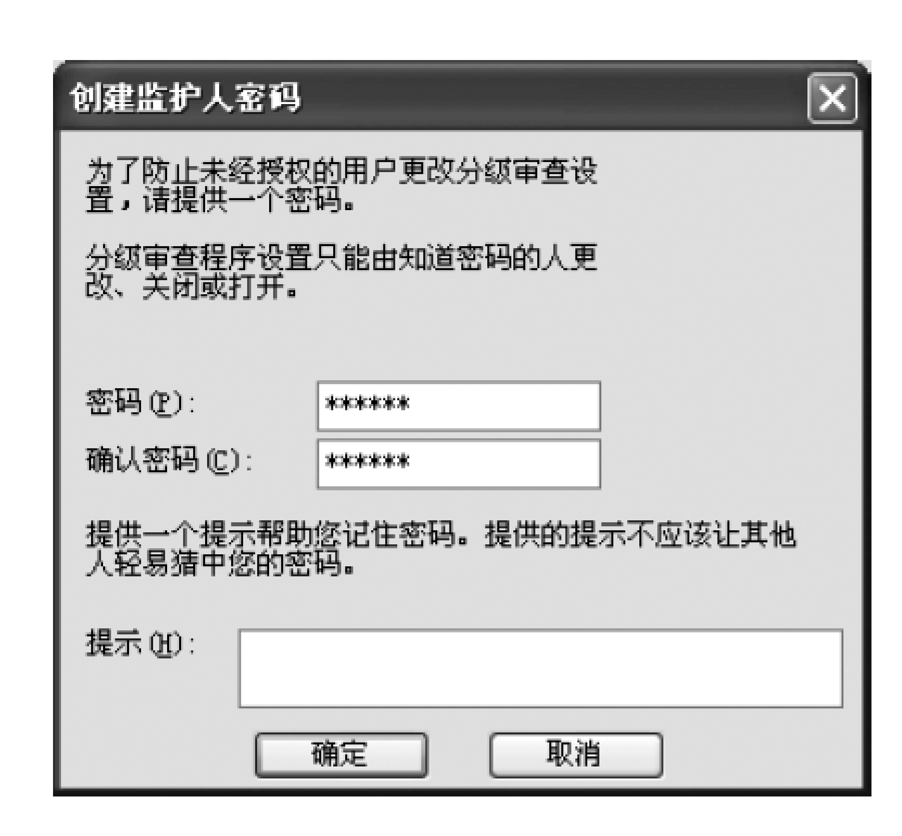


图 9.12 “创建监护人密码”对话框

9.4 Web 服务器的安全策略

9.4.1 制定安全策略

1. 定制安全政策

无论多么优秀的系统，必须有人的安全管理和合法地使用，否则就没有安全可言。安全政策包括以下几个方面。

(1) 定义安全资源,进行重要等级划分

这是为了从全局的观点制定安全策略。它是一项具体的工作,不同单位、不同的管理层对安全资源的定义各不相同。

(2) 进行安全风险评估

安全风险评估是权衡考虑各类安全资源的价值和对它们保护所需要的费用,尽量以适当的开销获得满意的安全保障。很明显,个人娱乐站点的安全投资要比网上银行站点的安全投资少得多。

(3) 制定安全策略的基本原则

在安全资源的等级划分和风险评估的基础上,制定安全策略的基本原则。每个站点的基本策略都是独一无二的,它为该站点定义预期的安全级别,就是说,该站点如何规划安全性。

(4) 建立安全培训制度

为增加单位员工的安全认识,从人为的角度尽量避免安全问题的发生,要建立安全培训制度。

(5) 具有意外事件处理措施

安全是相对的,不是绝对的。所以,必须明确无论安全措施如何完备,如何具体,还是有可能出现意外的安全问题,所以必须有相应的意外事件处理和补救的措施。

2. 认真组织 Web 服务器

服务器的安全策略有很多内容。这里简单说明几个重要的内容。

① 选择好合适的 Web 服务器设备和相关软件。

② 提供静态页面和多种动态页面的能力。

③ 接受和处理用户信息的能力。

④ 提供站点搜索服务的能力。

⑤ 远程管理的能力。

而关于安全方面的要求如下。

① 在已知的 Web 服务器漏洞中,针对该类型的最少。

② 对服务器的管理操作只能由授权用户执行。

③ 拒绝通过 Web 访问不公开的信息。

④ 能够禁止内嵌的不必要的网络服务。

⑤ 能够控制各种形式的可执行程序的访问。

⑥ 能够具有一定的容错性。

⑦ 能对某些 Web 操作进行日志记录,便于执行入侵监测和入侵企图分析。

(1) 仔细配置 Web 服务器

因为服务器的重要性,在它的配置上,一定要仔细,采用如下方法。

① 将服务器与内部网隔离开。Web 服务器被入侵的时候,会造成 Web 服务器系统被破坏甚至崩溃;入侵者收集如用户名、口令等信息;入侵者借助入侵的服务器为基础,进一步破坏其他网络等危害。

② 做好安全的 Web 站点的备份。备份系统是系统管理员必须做的一件事。通常，Web 服务器都采用多台备份机器在服务。但是要保证备份的内容是真实、可靠和备份存储的地方是可靠、安全的。

③ 合理配置主机系统。主机的操作系统是 Web 的平台，合理地配置主机系统，能够为 Web 服务器提供强大的安全支持。主要考虑仅仅提供必要的服务和使用必要的辅助工具。

④ 合理配置 Web 服务器软件。

（2）Web 服务器的安全管理

Web 服务器的相关内容要认真组织，其内容主要包括以下几个方面。

① 更新 Web 服务器内容尽量采用安全方式，比如，尽可能避免网络更新，而是采用本地方式。

② 经常审查有关日志。

③ 进行必要的数据备份。

备份是对付任何意外事故的保留方法，是系统最后的安全防线。

④ 定期对 Web 服务器进行安全检查。

安全检查的目的是为了及时发现 Web 服务器系统的安全缺陷和及时发现入侵痕迹。

3．了解最新的安全指南

了解最新的安全指南很重要，主要目的有以下几点。

① 及时更新系统软件和应用软件的版本，避免已存在漏洞的软件仍旧在使用。

② 了解最新发现的安全漏洞和新的攻击工具的特点，以便做好预防工作。

③ 了解、掌握最新的安全保护技术和工具。

④ 修订原来的安全策略，引进必要的安全工具。

每个网站的安全需求不同，受到攻击的几率和手段都不相同，因此，在实践中系统的安全工作要结合系统本身的特点来进行。

9.4.2 Web服务器安全应用

1．正确安装 Windows Server 2003

（1）分区和逻辑盘的分配

推荐的安全配置是建立 3 个逻辑驱动器，第一个大于 2GB，用来存放系统和重要的日志文件，第二个安装 IIS，第三个安装 FTP，这样无论 IIS 或 FTP 出了安全漏洞都不会直接影响到系统目录和系统文件。要知道，IIS 和 FTP 是对外服务的，比较容易出问题。而把 IIS 和 FTP 分开主要是为了防止入侵者上传程序并从 IIS 中运行。

（2）安装顺序的选择

Windows Server 2003 在安装中需要注意以下两点。

① 何时接入网络。Windows Server 2003 在安装时有一个漏洞，在输入 Administrator 密码后，系统就建立了 ADMIN＄的共享，但是并没有用刚刚输入的密码来保护它，这种

情况一直持续到再次启动后,在此期间,任何人都可以通过 ADMIN$ 进入你的机器;同时,只要安装一完成,各种服务就会自动运行,而这时的服务器是满身漏洞,非常容易进入的,因此,在完全安装并配置好 Windows Server 2003 之前,一定不要把主机接入网络。

② 补丁的安装。补丁的安装应该在所有应用程序安装完之后,因为补丁程序往往要替换/修改某些系统文件,如果先安装补丁再安装应用程序有可能导致补丁不能起到应有的效果,例如,IIS 的 HotFix 就要求每次更改 IIS 的配置都需要安装。

2. 安全配置 Windows Server 2003

即使正确地安装了 Windows Server 2003,系统还是有很多漏洞,还需要进一步进行细致的配置。

(1) 端口。端口是计算机和外部网络相连的逻辑接口,也是计算机的第一道屏障,端口配置正确与否直接影响到主机的安全,一般来说,仅打开需要使用的端口会比较安全,配置的方法是在网卡属性→TCP/IP→高级→选项→TCP/IP 筛选中启用 TCP/IP 筛选,不过对于 Windows Server 2003 的端口过滤来说,有一个不好的特性:只能规定打开哪些端口,不能规定关闭哪些端口,这样对于需要开大量端口的用户就不太方便。

(2) IIS。IIS 是微软的组件中漏洞最多的一个,平均两三个月就要出一个漏洞,而微软的 IIS 默认安装又不安全,所以 IIS 的配置是重点。

首先,把 C 盘那个 Inetpub 目录彻底删掉,在 D 盘新建一个 Inetpub,也可以给目录改一个名字,但是自己要记得,在 IIS 管理器中将主目录指向 D:\Inetpub。

其次,将 IIS 安装时默认的 Scripts 等虚拟目录一概删除,如果需要什么权限的目录可以以后慢慢建,需要什么权限即开放什么权限。

3. 账号安全

Windows Server 2003 的账号安全是另一个重点,首先,Windows Server 2003 的默认安装,允许任何用户通过空用户得到系统所有账号/共享列表,这个本来是为了方便局域网用户共享文件的,但是一个远程用户也可以得到用户列表并使用暴力法破解用户密码。Windows Server 2003 的本地安全策略(如果是域服务器就是在域服务器安全和域安全策略中)有这样的选项 RestrictAnonymous(匿名连接的额外限制),这个选项有如下 3 个值。

0:None. Rely on default permissions(无,取决于默认的权限)。

1:Do not allow enumeration of SAM accounts and shares(不允许枚举 SAM 账户和共享)。

2:No access without explicit anonymous permissions(没有显式匿名权限就不允许访问)。

值 0 这个值是系统默认的,什么限制都没有,远程用户可以知道你机器上所有的账户、组信息、共享目录、网络传输列表(NetServerTransportEnum)等,对服务器来说这样的设置非常危险。

值 1 只允许非 NULL 用户存取 SAM 账户信息和共享信息。

值 2 在 Windows Server 2003 中才支持的，推荐设为 1 比较好。

这样，入侵者现在没有办法拿到用户列表，应该说账户安全了。另外，为了安全还要将系统内建的 Administrator 改名。

4. 设置好安全策略

设置策略和设置方法可参照操作系统安全这一部分的内容。

5. 目录和文件权限

为了控制好服务器上用户的权限，同时也为了预防以后可能的入侵和溢出，还必须非常小心地设置目录和文件的访问权限。

实际上，Web 的安全和应用在很多时候是矛盾的，因此，需要在其中找到平衡点，毕竟服务器是给用户使用的，如果安全原则妨碍了系统应用，那么这个安全原则也不是一个好的原则。

网络安全是一项系统工程，它不仅有空间的跨度，还有时间的跨度。很多用户（包括部分系统管理员）认为进行了安全配置的主机就是安全的，其实这其中有个误区：我们只能说一台主机在一定的情况一定的时间上是安全的，随着网络结构的变化、新的漏洞的发现，管理员/用户的操作，主机的安全状况是随时随地变化着的，只有让安全意识和安全制度贯穿整个过程才能做到真正的安全。



【案例】 Web 服务器安全配置

案例分析

Web 服务器创建好，还需要进行适当的管理才能使用户的信息安全、有效地被其他访问者访问。

操作环境

安装了 Windows Server 2003 操作系统的服务器。

操作步骤

第 1 步 启用过期内容。

启用过期内容就是指通过设置来保证自己站点的过期信息不被发布出去。

(1) 选择“HTTP 头”选项卡，如图 9.13 所示。在该选项卡中，选中“启用内容过期”复选框，激活“启用内容过期”选项区域中的选项。

(2) 在“启用内容过期”选项区域中，用户可以设置内容的过期时间。

第 2 步 内容分级设置。

如果用户站点的内容并不是针对所有的访问者，需要进行内容分级设置，以防止不具备分级要求的其他访问者查看站点内容。在预设的情况下，Windows Server 2003 启用

的是 RSAC(Recreational Software Advisory Council)分级服务系统进行分级服务。该 Internet 分级是斯坦福大学的 Donald F. Roberts 博士研究的，它主要针对暴力、性、裸体和语言 4 个方面进行分级设置。在设置分级服务内容之前，用户需要上网填写一个 RSAC 分级问卷，以获得一些推荐的内容分级，以便更好地进行分级设置。分级内容设置过程如下。

(1) 在图 9.13 中，单击“编辑分级”按钮，打开“内容分级”对话框，如图 9.14 所示。



图 9.13 “HTTP 头”选项卡



图 9.14 “内容分级”对话框

(2) 对 RSAC 系统有所了解之后，用户就可以设置分级服务的内容，以过滤公司的

Web 页的内容。单击“分级”选项卡，并选择“对此内容启用分级”复选框，如图 9.15 所示。

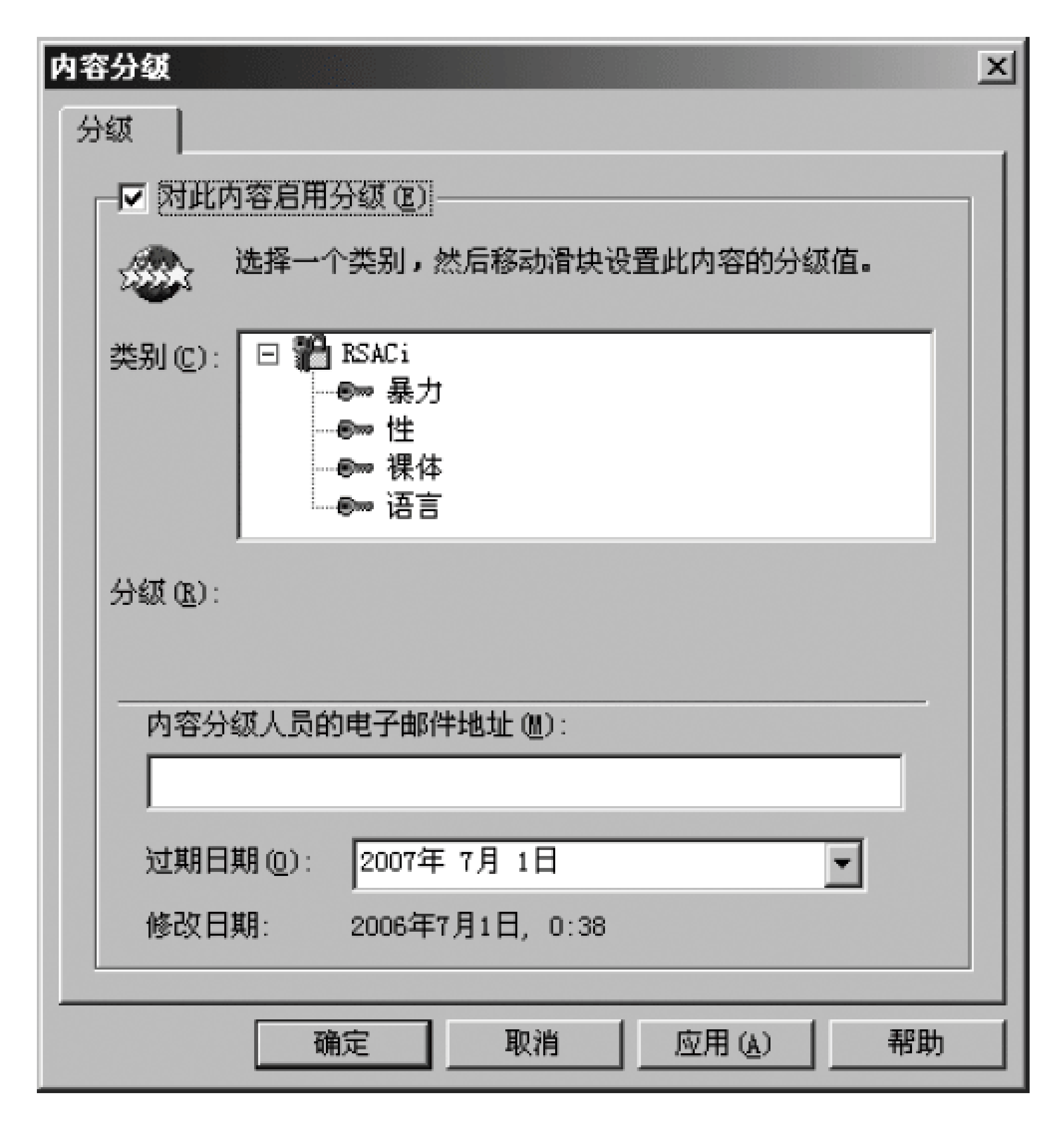


图 9.15 “分级”选项卡

(3) 在“类别”列表框中，选择暴力、性、裸体和语言 4 个类别中的一种，分级滑块就会显示出来，调节该滑块，可改变所选类别的分级级别。

(4) 如果希望对自己的电子邮件进行分级服务，用户可以在“内容分级人员的电子邮件地址”文本框中输入自己的电子邮件地址。

(5) 如果希望单独为分级服务设置失效时间，可单击“过期日期”下拉列表框中的下三角按钮，从弹出的电子日历中选择一个日期。

(6) 设置好之后，单击“确定”按钮返回“默认网站 属性”对话框，再单击“确定”按钮，保存设置。

第 3 步 添加网页页脚。

在 Web 站点管理中，用户经常在每一个 Web 页的前面插入一个由 HTML 语言编写的脚本文件，作为网页页脚，以增加 Web 站点的内容。

(1) 创建一个 HTML 网页页脚文件，并把它保存在自己的 Web 服务器所在的硬盘上。

(2) 在 Internet 服务管理器的控制台目录树中，右击某一个 Web 站点或者目录子节点，例如，msadc 虚拟目录，从快捷菜单中选择“属性”命令，打开“msadc(停止)属性”对话框，选择“文档”选项卡，如图 9.16 所示。

(3) 选择“启用文档页脚”复选框；在“启用文档页脚”文本框中输入页脚文件的完整路径。如果用户不知道页脚文件的完整路径，可单击“浏览”按钮，打开“打开”对话框进行选择。

(4) 单击“确定”按钮，返回到图 9.16 所示的对话框，再单击“确定”按钮保存设置。

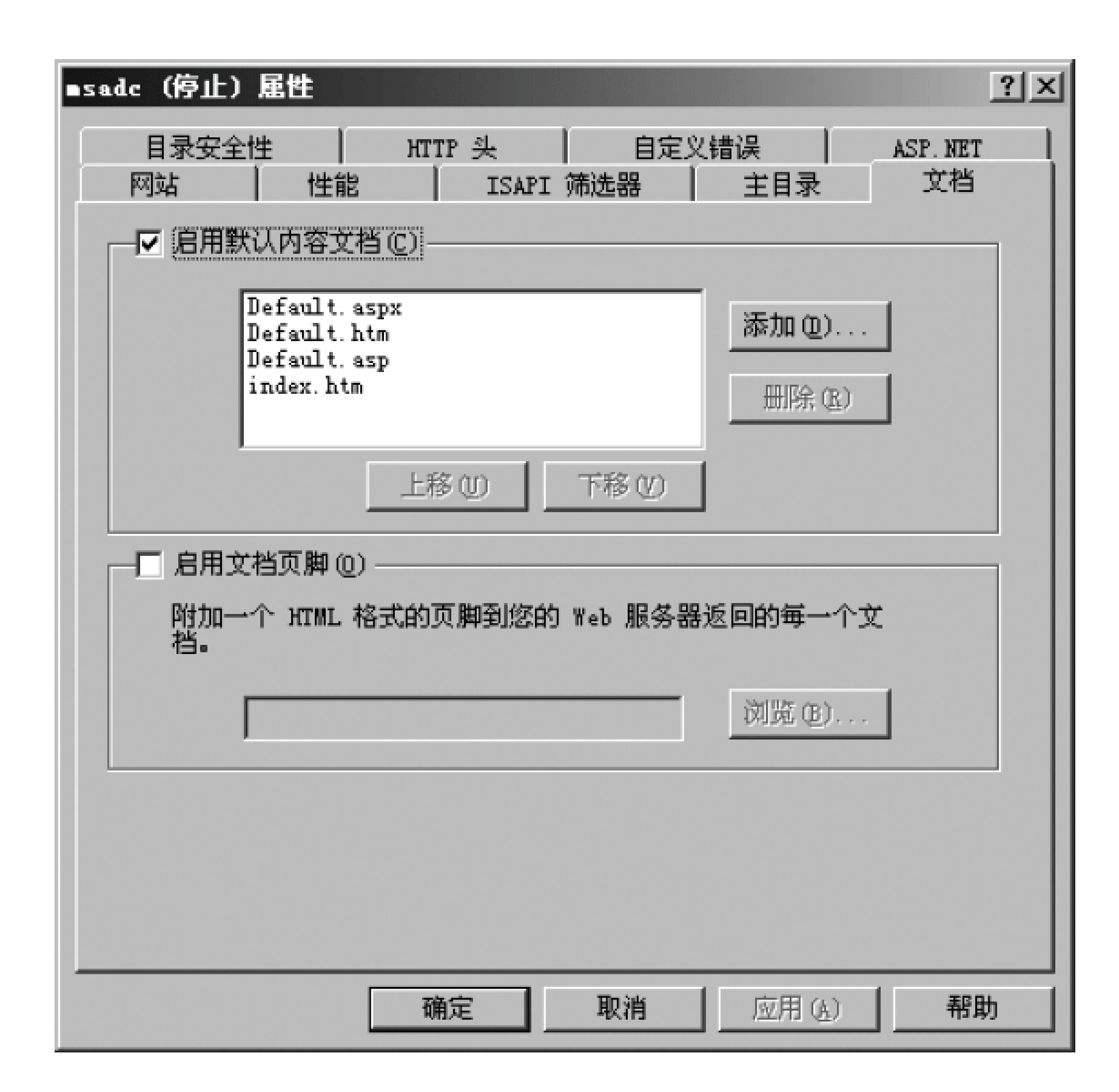


图 9.16　“文档”选项卡

第 4 步　安全与权限设置。

安全与权限设置是 IIS 保证其站点安全的最重要的保护措施，它可用来控制怎样验证用户的身份及他们的访问权限。

(1) 选择“所有任务”→“权限向导”命令，打开“权限向导”窗口。单击“下一步”按钮，打开“安全设置”页面，如图 9.17 所示。

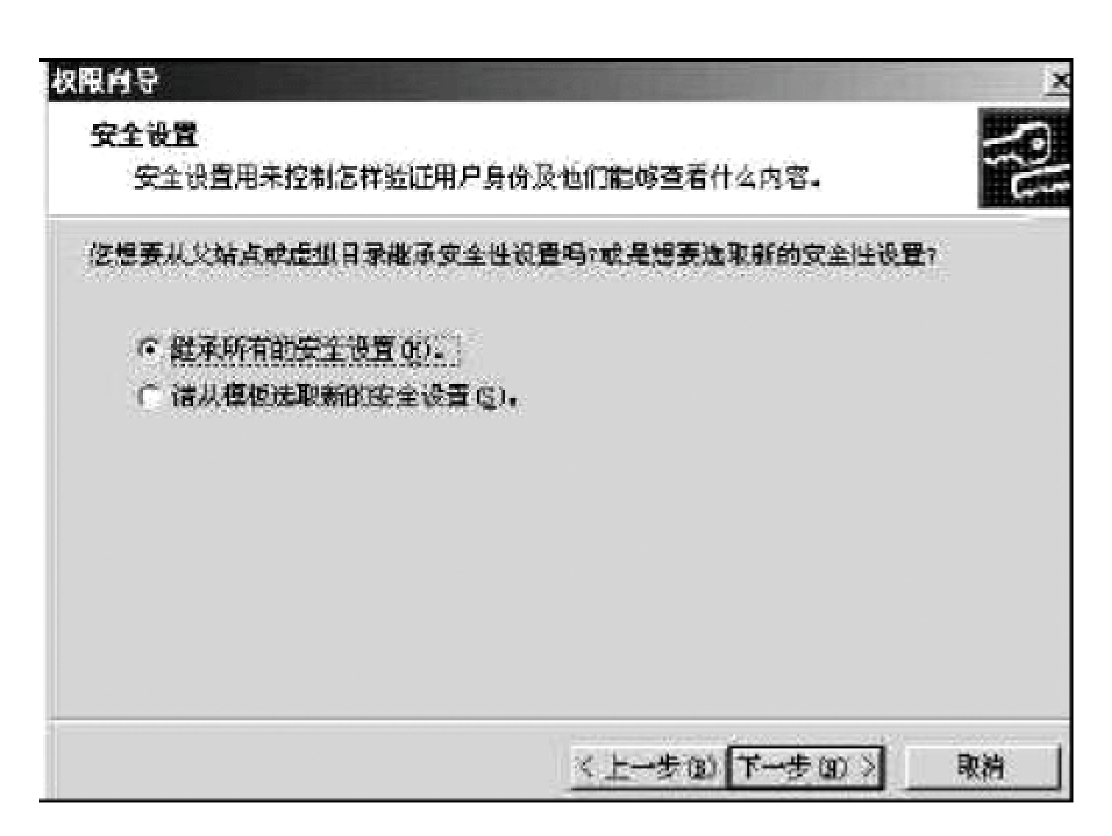


图 9.17　“安全设置”页面

(2) 如果要从父站点或者虚拟目录继承安全性设置，应选择“继承所有的安全设置”单选按钮；如果需要选取新的安全性设置，应选择“请从模板选取新的安全设置”单选按钮。

(3) 单击“下一步”按钮，打开“ Windows 目录和文件权限”页面，如图 9.18 所示。

(4) 如果要保持 Windows 目录和文件权限，应选择“保持目录和文件权限”单选按钮；如果要保持原来 Windows 目录和文件权限并加入新设置的权限，应选择“原封不动地

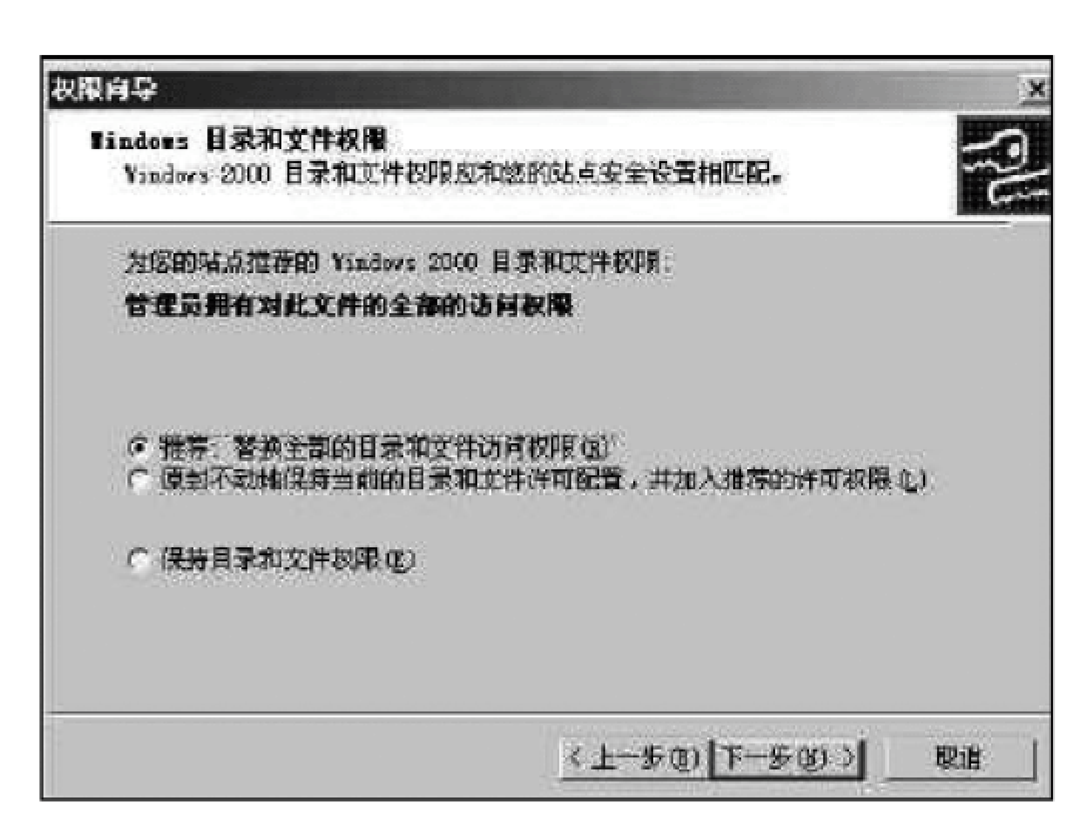


图 9.18 “Windows 目录和文件权限”页面

保持当前的目录和文件许可配置,并加入推荐的许可权限”单选按钮。这里选择“推荐:替换全部的目录和文件访问权限”单选按钮,以新设置的权限替换原有的目录和文件权限。

(5) 单击“下一步”按钮,打开如图 9.19 所示的“安全摘要”页面,在列表框中选择要应用的设置,包括验证方法、访问许可、IP 地址限制和文件 ACL 将不能被修改等设置。

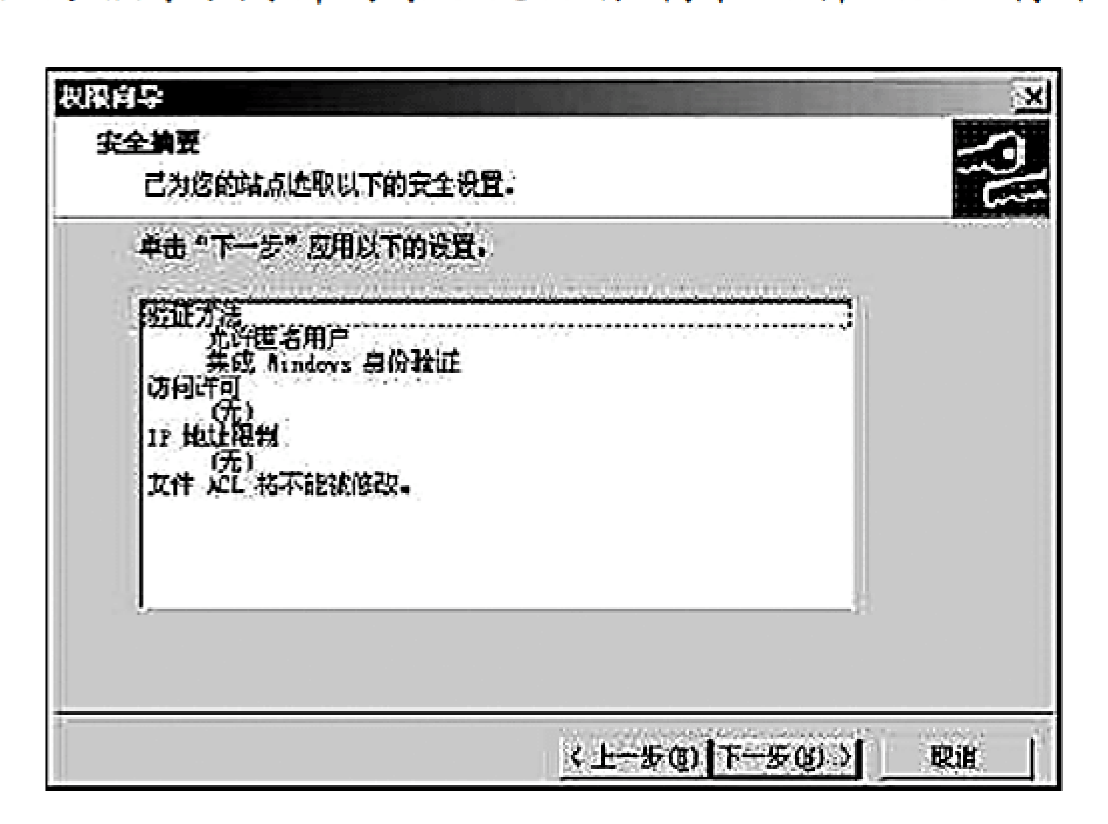


图 9.19 “安全摘要”页面

(6) 单击“下一步”按钮,打开“您已成功地完成 IIS 5.0‘权限向导’”窗口,再单击“完成”按钮即可完成设置。

第 5 步 安全认证。

在 Windows Server 2003 中,对于通过 HTTP 协议访问,Internet 信息服务提供了 3 种登录认证方式,它们分别是匿名方式、明文方式和询问/应答方式。用户采用哪种方式取决于用户建立 Internet 信息服务器的目的。

由于在许多 Internet 信息服务器上,对 Web、FTP 及 SMTP 虚拟服务器的访问都是匿名的,下面以匿名访问为例介绍如何进行安全认证设置。

(1) 在如图 9.20 所示的对话框中,选择“目录安全性”选项卡。

(2) 在“身份验证和访问控制”选项组中,单击“编辑”按钮,打开“身份验证方法”对话

框,如图 9.21 所示。



图 9.20 “目录安全性”选项卡

图 9.21 设置匿名访问和验证控制

(3) 要选择匿名认证方式,选中“启用匿名访问”复选框,并单击“浏览”按钮,打开如图 9.22 所示的“选择用户”对话框进行设置。

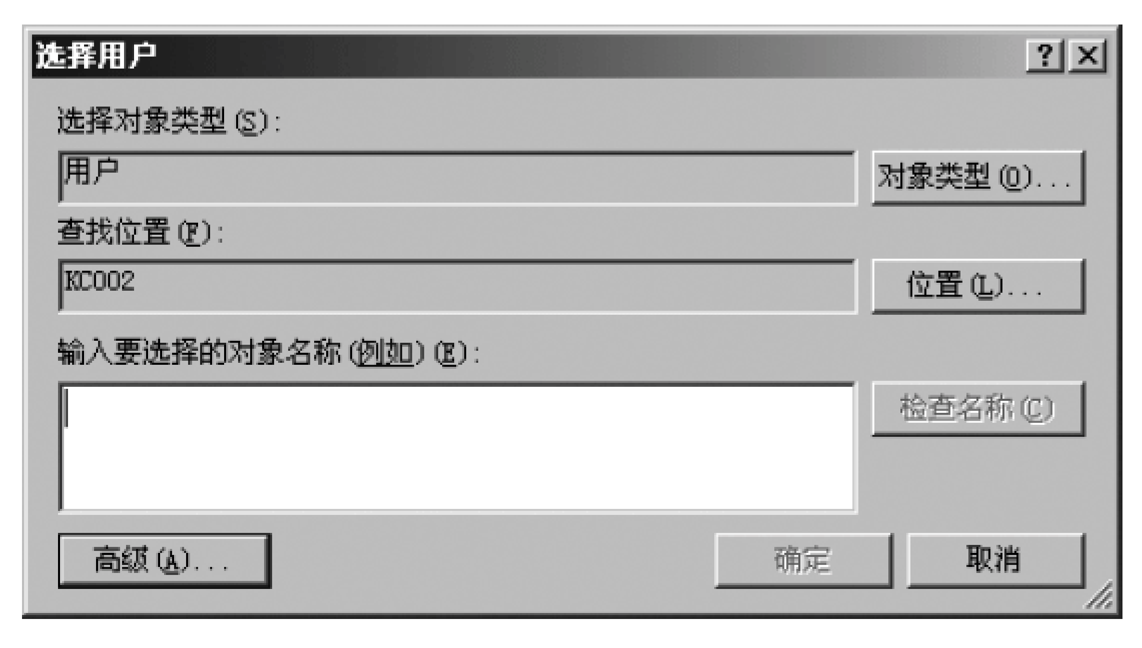


图 9.22 设置匿名账号

(4) 在安装 Internet 信息服务时,系统将自动创建一个匿名账号:IUSR 计算机名,如果计算机名为 KC002,则匿名账号为 IUSR_KC002。使用“IUSR 计算机名”账号可以将 Web 客户登录到服务器上。允许匿名服务时,管理员可更改用户匿名请求的用户账号,并可更改此账号的密码。在“用户名”文本框中直接输入用户账号名,或者单击“浏览”按钮,打开如图 9.23 所示的“对象类型”对话框,在此选择一个要添加的用户账号。

(5) 在“身份验证方法”对话框中,在“密码”文本框中输入用户的密码。

(6) 单击“确定”按钮完成匿名访问设置,直至返回“默认网站 属性”对话框,然后单击“确定”按钮关闭对话框。

第 6 步 IP 地址及域名限制。

通过 IP 地址及域名限制,用户可禁止某些特定的计算机或者某些区域中的主机对自



图 9.23　选择 Windows 用户账号

己的 Web 和 FTP 站点及 SMTP 虚拟服务器的访问。当有大量的攻击和破坏来自于某些地址或者某个子网时，使用这种限制机制是非常有用的。不过，进行 IP 地址及域名限制的首要条件是用户必须知道网络黑客的计算机使用哪些 IP 地址或属于哪些网络区域，否则无法进行限制。对基于 Internet 的信息服务器，站点接受来自于各方的访问，用户很难进行地址限制。一般，只有基于企业内部网络的信息服务器才使用 IP 地址和域名进行安全保护。下面以 Web 站点为例进行 IP 地址和域名限制的设置过程。

(1) 在图 9.20 中，在"IP 地址和域名限制"选项组中单击"编辑"按钮，打开"IP 地址和域名限制"对话框，如图 9.24 所示。

(2) 如果选择"授权访问"单选按钮，除了"下例除外"列表框中的计算机外，其他所有的计算机都可访问该 Web 站点上的内容。如果选择"拒绝访问"单选按钮，除了"下例除外"列表框中的计算机外，其他所有的计算机都不能访问该 Web 站点上的内容。这里选择"授权访问"单选按钮并添加没有访问权限的计算机。

(3) 单击"添加"按钮，打开"拒绝访问"对话框，如图 9.25 所示。



图 9.24　设置 IP 地址和域名限制

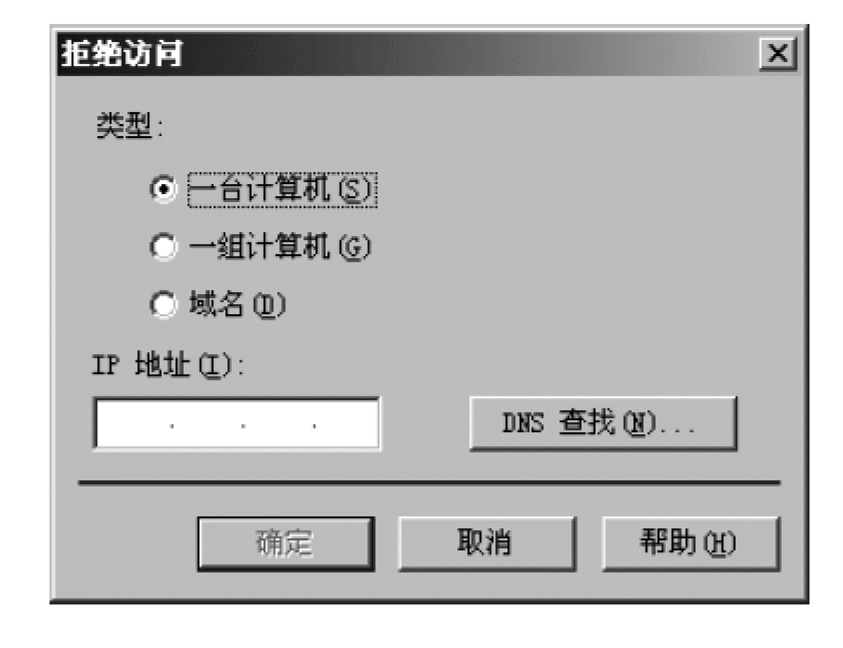


图 9.25　拒绝访问设置

(4) 如果要对单个计算机进行限制，选择"一台计算机"单选按钮，并在"IP 地址"文本框中输入要授权的计算机的 IP 地址；或者单击"DNS 查找"按钮，打开"DNS 查找"对话框，选择某个 DNS 域中要拒绝的计算机。如果要对一组计算机进行限制，选择"一组计算机"单选按钮，在"网络标识"文本框中输入要授权的一组计算机中的任何一个计算机的 IP 地址，并在"子网掩码"文本框中输入子网掩码。如果要对某个域中的计算机进行限制，选择"域名"单选按钮，并在"域名"文本框中输入拒绝的域的域名。

(5) 单击"确定"按钮返回到"IP 地址和域名限制"对话框。如果还要进行访问授权，可继续单击"添加"按钮进行添加。这样，被添加的单个计算机、一组计算机或者一个域的客户被拒绝访问服务器，而其他的客户则有访问权。

(6) 单击"确定"按钮返回到"默认网站 属性"对话框，再单击"确定"按钮保存设置。

第 7 步　停止、启动和暂停站点服务。

在站点维护中，停止、启动和暂停站点服务是经常要进行的工作。例如，当某个站点的内容和设置需要进行比较大的修改时，用户可将该站点的服务停止或者暂停，以便操作。当已经停止或暂停的站点需要启动自己的服务时，就启动它。

要停止、启动和暂停某个站点的信息服务，在控制台目录树中，展开"Internet 信息服务"节点和服务器节点，展开服务器节点。如果要暂停某个 Web 或者 FTP 站点服务，右击该站点，从快捷菜单中选择"暂停"命令即可；如果要停止某个 Web 或者 FTP 站点服务，右击该站点，从快捷菜单中选择"停止"命令即可；如果要启动某个已经暂停或者停止的 Web 或者 FTP 站点服务，右击该站点，从快捷菜单中选择"启动"命令即可。

本 章 小 结

Web 是 Internet 上发展最快同时又是使用最多的一项服务，它可以提供包括文本、图形、声音和视频等在内的多媒体信息。

Web 的安全有很多因素需要考虑，如 Web 服务器的安全，Web 服务器所在的网络安全，Web 浏览器的用户的安全风险等。

本 章 练 习

一、填空题

1. WWW 服务采用客户机/服务器工作模式，它以________与超文本传输协议为基础，为用户提供界面一致的信息浏览系统。
2. HTTP 协议是分布式的 Web 应用的核心技术协议，在 TCP/IP 协议栈中属于________层协议。
3. 目前常用的 Web 浏览器主要有________和________两种。
4. Web 浏览器的不安全因素主要来自________。
5. Web 欺骗攻击是指________。

二、选择题

1. 在访问 Internet 的过程中，为了防止 Web 页面中恶意代码对自己计算机的损害，可以采取________防范措施。

A. 利用 SSL 访问 Web 站点

B. 将要访问的 Web 站点按其可信度分配到浏览器的不同安全区域

C. 在浏览器中安装数字证书

D. 要求 Web 站点安装数字证书

2. 统一的安全电子政务平台包括统一的可信 Web 服务平台、统一的 Web 门户平台与统一的________。

A. 数据交换平台　　B. 电视会议平台

C. 语音通信平台　　D. 电子邮件平台

三、简答题

1. Web 服务器的安全需求有哪些?
2. Web 浏览器的安全需求有哪些?
3. 简述 Web 服务器的安全策略。
4. 如何进行服务器的安全配置?

实训　IE 浏览器的安全设置

实训目的

(1) 了解 IE 浏览器的基本功能。

(2) 掌握提高 IE 浏览器安全性的设置方法。

实训环境

(1) 一台连上 Internet 的计算机。

(2) IE 8.0 浏览器。

实训步骤

第 1 步　IE 浏览器安全性的设置。

有很多针对 IE 浏览器的病毒都是通过在网页中使用恶意脚本程序来运行的,只需要禁止在浏览器中执行这些脚本就可以达到防患于未然的目的。

在 IE 浏览器中选择"工具"→"Internet 选项"命令打开"Internet 属性"对话框,打开"安全"选项卡,如图 9.26 所示。

单击"自定义级别"按钮,弹出"安全设置-Internet 区域"对话框,如图 9.27 所示。将"脚本"选项中的"Java 小程序脚本"和"活动脚本"都设置成"禁用",以便以后上网浏览时不必担心脚本类病毒。不过,这也使得正常网页中所有通过脚本实现的网页特殊效果也全部被禁用。



图 9.26 “安全”选项卡



图 9.27 “安全设置-Internet”对话框

第 2 步 清除 IE 操作的痕迹。

在用户上网冲浪时，IE 会自动产生一些临时文件、垃圾文件和记录一些信息，在很多情况下这些痕迹也能暴露用户隐私信息。

(1) 删除 Internet 临时文件

选择 IE 上“工具”→“Internet 选项”，打开“Internet 选项”对话框的“常规”选项卡，单击“删除”按钮。在弹出的“删除浏览的历史记录”对话框中选中“Internet 临时文件”复选框，单击“删除”按钮，如图 9.28 所示。

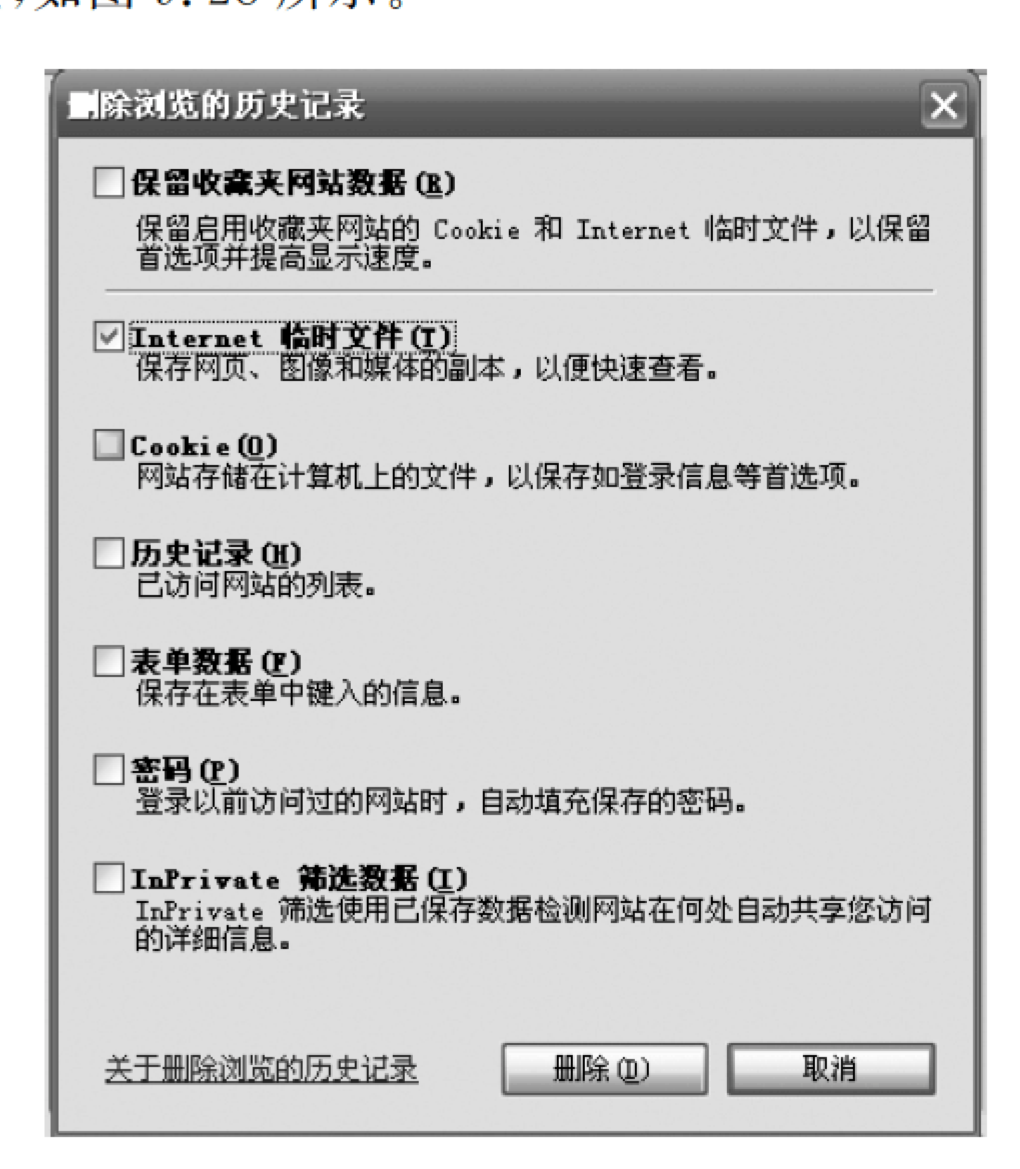


图 9.28 “删除文件”对话框

(2) 清除 IE 的历史记录

打开“Internet 选项”对话框，选择 IE 上“工具”→“Internet 选项”，打开 “Internet 选项”对话框的“常规”选项卡，单击“删除”按钮，在弹出的“删除浏览的历史记录”对话框中选中“历史记录”复选框，单击“删除”按钮。

(3) 清除访问过的网站地址

在“Internet 选项”对话框中选择“内容”选项卡，单击“设置”按钮，如图 9.29 所示。然后，在弹出“自动完成设置”对话框中不勾选“地址栏”复选框，如图 9.30 所示。这样就无法通过使用部分地址匹配的方法打开曾经访问过的 Web 站点。

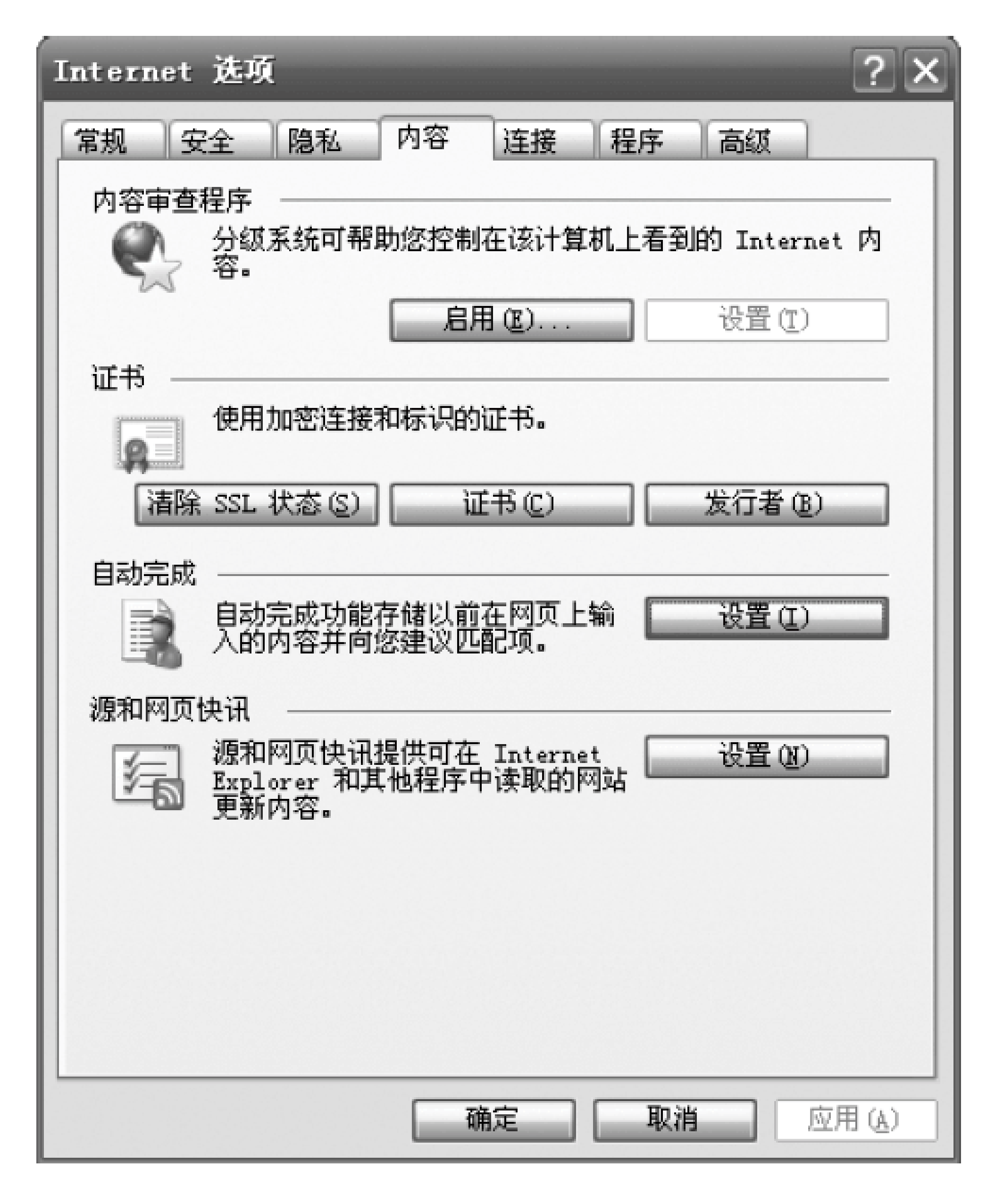


图 9.29 “内容”选项卡

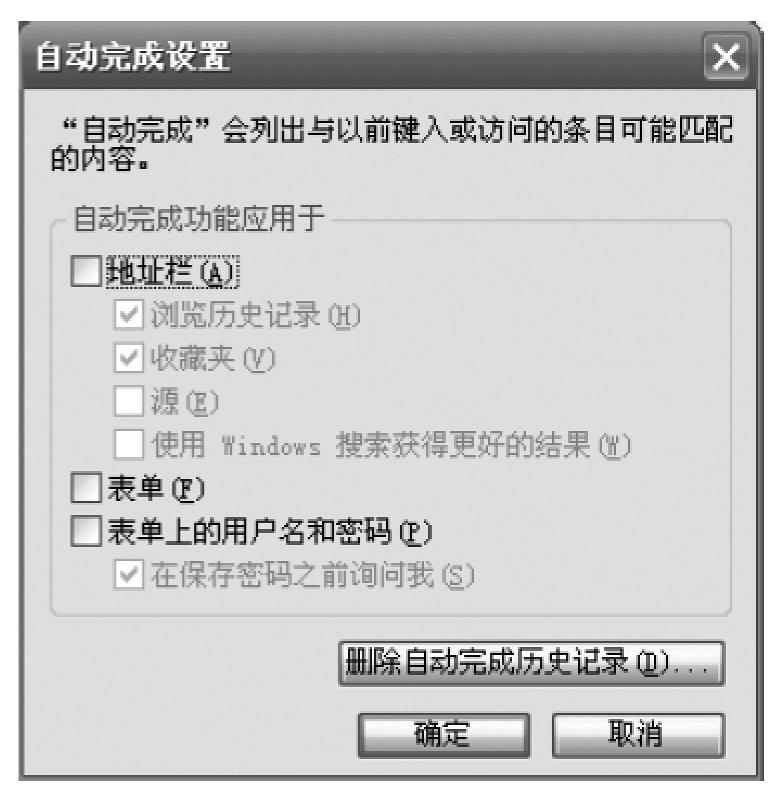


图 9.30 “自动完成设置“对话框

(4) 清除 IE 记住的表单的密码和表单

打开 “Internet 选项”对话框的“常规”选项卡，单击“删除”按钮，然后在弹出的“删除浏览的历史记录”对话框中选中“表单数据”和“密码”复选框，“删除”按钮确认，如图 9.31 所示。

第 3 步 禁用 Cookie。

Cookie 是一种发送到客户浏览器的文本串名柄，并保存在客户机硬盘上，很容易暴露用户信息，会给自己带来安全隐患。通过以下操作可以禁用 Cookie。

选择“工具”→“Internet 内容”命令，选择“安全”选项卡，如图 9.26 所示。在“选择要查看的区域或更改安全设置”列表框中选择 Internet 图标。然后，单击对话框中的“自定义级别”按钮，打开“安全设置-Internet 区域”对话框，在“设置”选项组中，把“允许使用存储在计算机上的 Cookie”和“允许使用每个对话 Cookie”这两个选项分别设为“禁用”。用同样的方法，在“安全”选项卡的“本地 Internet”、“可信站点”和“受限站点”图标，并分别禁止在这些站点使用 Cookie。以后系统碰到有 Cookie 请求时一律加以拒绝。



图 9.31 清除表单对话框

参 考 文 献

[1] 蔡立军.计算机网络安全技术[M].北京:中国水利水电出版社,2002.
[2] 方勇,刘嘉勇.信息安全导论[M].北京:电子工业出版社,2003.
[3] 高鹏,严望佳.构建安全的 Web 站点[M].北京:清华大学出版社,1999.
[4] 顾巧论.计算机网络安全[M].北京:科学出版社,2003.
[5] 黄允聪.网络安全基础[M].北京:清华大学出版社,2001.
[6] 蒋建春,冯登国.网络入侵检测系统的设计与实现[M].北京:电子工业出版社,2002.
[7] 焦树海.计算机安全概论[M].天津:南开大学出版社,2004.
[8] 李海泉,李健.计算机系统安全技术[M].北京:人民邮电出版社,2001.
[9] 宋红.计算机安全技术[M].北京:中国铁道出版社,2003.
[10] 唐正军.网络入侵检测系统的设计与实现[M].北京:电子工业出版社,2002.
[11] 新时代工作室.网络安全与黑客[M].青岛:青岛出版社,2000.
[12] 徐卓峰.信息安全技术[M].武汉:武汉理工大学出版社,2004.
[13] 袁家政.计算机系统安全与应用技术[M].北京:清华大学出版社,2002.
[14] 张小斌.计算机网络安全工具[M].北京:清华大学出版社,1999.
[15] 张永平.计算机系统安全技术[M].北京:高等教育出版社,2003.
[16] 钟乐海.网络安全技术[M].北京:电子工业出版社,2001.
[17] 刘远生,辛一.计算机网络安全[M].北京:清华大学出版社,2009.
[18] 归奕红,刘宁. 网络安全技术案例教程[M].北京:清华大学出版社,2010.